Red Hat Enterprise Linux 6

6.2 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 6.2

Edition 2

Last Updated: 2017-10-24

Red Hat Enterprise Linux 6 6.2 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 6.2
Edition 2

Red Hat Engineering Content Services

Legal Notice

Abstract

The Red Hat Enterprise Linux 6.2 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications between Red Hat Enterprise Linux 6.1 and minor release Red Hat Enterprise Linux 6.2.

Table of Contents

PREFACE

The *Red Hat Enterprise Linux 6.2 Technical Notes* list and document the changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 6.1 and minor release Red Hat Enterprise Linux 6.2.

For system administrators and others planning Red Hat Enterprise Linux 6.2 upgrades and deployments, the Technical Notes provide a single, organized record of the bugs fixed in, features added to, and Technology Previews included with this new release of Red Hat Enterprise Linux.

For auditors and compliance officers, the *Red Hat Enterprise Linux 6.2 Technical Notes* provide a single, organized source for change tracking and compliance testing.

For every user, the *Red Hat Enterprise Linux 6.2 Technical Notes* provide details of what has changed in this new release.

NOTE

The Package Manifest is available as a separate document.

CHAPTER 1. TECHNOLOGY PREVIEWS

Technology Preview features are currently not supported under Red Hat Enterprise Linux subscription services, may not be functionally complete, and are generally not suitable for production use. However, these features are included as a customer convenience and to provide the feature with wider exposure.

Customers may find these features useful in a non-production environment. Customers are also free to provide feedback and functionality suggestions for a Technology Preview feature before it becomes fully supported. Errata will be provided for high-severity security issues.

During the development of a Technology Preview feature, additional components may become available to the public for testing. It is the intention of Red Hat to fully support Technology Preview features in a future release.

1.1. STORAGE AND FILE SYSTEMS

Parallel NFS

Parallel NFS (pNFS) is a part of the NFS v4.1 standard that allows clients to access storage devices directly and in parallel. The pNFS architecture eliminates the scalability and performance issues associated with NFS servers in deployment today.

pNFS supports 3 different storage protocols or layouts: files, objects and blocks. The Red Hat Enterprise Linux 6.2 NFS client supports the files layout protocol.

To automatically enable the pNFS functionality, create the **`/etc/modprobe.d/dist-nfsv41.conf`** file with the following line and reboot the system:

```
alias nfs-layouttype4-1 nfs_layout_nfsv41_files
```

Now when the **`-o minorversion=1`** mount option is specified, and the server is pNFS-enabled, the pNFS client code is automatically enabled.

For more information on pNFS, refer to http://www.pnfs.com/.

Open multicast ping (Omping), BZ#657370

Open Multicast Ping (Omping) is a tool to test the IP multicast functionality, primarily in the local network. This utility allows users to test IP multicast functionality and assists in the diagnosing if an issues is in the network configuration or elsewhere (that is, a bug). In Red Hat Enterprise Linux 6 Omping is provided as a Technology Preview.

Matahari

Matahari provides a set of Application Programming Interfaces (APIs) for operating systems management for remote access over QMF/QPID. Matahari in Red Hat Enterprise Linux 6.2 is fully supported only for Intel 64 and AMD64 architectures. Builds for other architectures are considered a Technology Preview.

System Information Gatherer and Reporter (SIGAR)

The System Information Gatherer and Reporter (SIGAR) is a library and command-line tool for accessing operating system and hardware level information across multiple platforms and programming languages. In Red Hat Enterprise Linux 6.2, SIGAR is considered a Technology Preview package.

fsfreeze

Red Hat Enterprise Linux 6 includes **fsfreeze** as a Technology Preview. **fsfreeze** is a new command that halts access to a file system on a disk. **fsfreeze** is designed to be used with hardware RAID devices, assisting in the creation of volume snapshots. For more details on the **fsfreeze** utility, refer to the `fsfreeze(8)` man page.

DIF/DIX support

DIF/DIX, is a new addition to the SCSI Standard and a Technology Preview in Red Hat Enterprise Linux 6. DIF/DIX increases the size of the commonly used 512-byte disk block from 512 to 520 bytes, adding the Data Integrity Field (DIF). The DIF stores a checksum value for the data block that is calculated by the Host Bus Adapter (HBA) when a write occurs. The storage device then confirms the checksum on receive, and stores both the data and the checksum. Conversely, when a read occurs, the checksum can be checked by the storage device, and by the receiving HBA.

The DIF/DIX hardware checksum feature must only be used with applications that exclusively issue ***O_DIRECT*** I/O. These applications may use the raw block device, or the XFS file system in ***O_DIRECT*** mode. (XFS is the only file system that does not fall back to buffered I/O when doing certain allocation operations.) Only applications designed for use with ***O_DIRECT*** I/O and DIF/DIX hardware should enable this feature.

For more information, refer to section *Block Devices with DIF/DIX Enabled* in the Storage Administration Guide

File system in user space

Filesystem in Userspace (FUSE) allows for custom file systems to be developed and run in user space.

Btrfs, BZ#614121

Btrfs is under development as a file system capable of addressing and managing more files, larger files, and larger volumes than the ext2, ext3, and ext4 file systems. Btrfs is designed to make the file system tolerant of errors, and to facilitate the detection and repair of errors when they occur. It uses checksums to ensure the validity of data and metadata, and maintains snapshots of the file system that can be used for backup or repair. The btrfs Technology Preview is only available on AMD64 and Intel 64 architectures.

WARNING

Red Hat Enterprise Linux 6 includes Btrfs as a technology preview to allow you to experiment with this file system. You should not choose Btrfs for partitions that will contain valuable data or that are essential for the operation of important systems.

LVM Application Programming Interface (API)

Red Hat Enterprise Linux 6 features the new LVM application programming interface (API) as a Technology Preview. This API is used to query and control certain aspects of LVM.

LVM RAID support, BZ#729712

In Red Hat Enterprise Linux 6.2, support for MD's RAID personalities has been added to LVM as a *Technology Preview*. The following basic features are available: create, display, rename, use, and remove RAID logical volumes. Automated fault tolerance is not yet available.

FS-Cache

FS-Cache is a new feature in Red Hat Enterprise Linux 6 that enables networked file systems (e.g. NFS) to have a persistent cache of data on the client machine.

eCryptfs File System

eCryptfs is a stacked, cryptographic file system. It is transparent to the underlying file system and provides per-file granularity. eCryptfs is provided as a Technology Preview in Red Hat Enterprise Linux 6.

1.2. NETWORKING

vios-proxy, BZ#721119

vios-proxy is a stream-socket proxy for providing connectivity between a client on a virtual guest and a server on a Hypervisor host. Communication occurs over virtio-serial links.

IPv6 support in IPVS

The IPv6 support in IPVS (IP Virtual server) is considered a Technology Preview.

1.3. CLUSTERING

Support for redundant ring for standalone Corosync, BZ#722469

Red Hat Enterprise Linux 6.2 introduces support for redundant ring with autorecovery feature as a Technology Preview. Refer to Section 2.7, “Clustering” for a list of known issues associated with this Technology Preview.

corosync-cpgtool, BZ#688260

The **corosync-cpgtool** now specifies both interfaces in a dual ring configuration. This feature is a Technology Preview.

Disabling rgmanager in /etc/cluster.conf, BZ#723925

As a consequence of converting the `/etc/cluster.conf` configuration file to be used by **pacemaker**, **rgmanager** must be disabled. The risk of not doing this is high; after a successful conversion, it would be possible to start **rgmanager** and **pacemaker** on the same host, managing the same resources.

Consequently, Red Hat Enterprise Linux 6.2 includes a feature (as a Technology Preview) that forces the following requirements:

- **rgmanager** must refuse to start if it sees the `<rm disabled="1">` flag in `/etc/cluster.conf`.
- **rgmanager** must stop any resources and exit if the `<rm disabled="1">` flag appears in `/etc/cluster.conf` during a reconfiguration.

pacemaker, BZ#456895

Pacemaker, a scalable high-availability cluster resource manager, is included in Red Hat Enterprise Linux 6 as a Technology Preview. Pacemaker is not fully integrated with the Red Hat cluster stack.

1.4. SECURITY

TPM

TPM hardware can create, store and use RSA keys securely (without ever being exposed in memory), verify a platform's software state using cryptographic hashes and more. The user space libraries, trousers and tpm-tools, are considered a Technology Preview.

1.5. DEVICES

Brocade BFA driver

The Brocade BFA driver is considered a Technology Preview feature in Red Hat Enterprise Linux 6. The BFA driver supports Brocade FibreChannel and FCoE mass storage adapters.

SR-IOV on the be2net driver, BZ#602451

The SR-IOV functionality of the Emulex **`be2net`** driver is considered a Technology Preview in Red Hat Enterprise Linux 6.

1.6. KERNEL

Support for Fiber Channel over Ethernet (FCoE) target mode

Red Hat Enterprise Linux 6.2 includes support for Fiber Channel over Ethernet (FCoE) target mode as a *Technology Preview*. This kernel feature is configurable via **targetadmin**, supplied by the fcoe-target-utils package. FCoE is designed to be used on a network supporting Data Center Bridging (DCB). Further details are available in the **`dcbtool(8)`** and **`targetadmin(8)`** man pages.

IMPORTANT

This feature uses the new SCSI target layer, which falls under this Technology Preview, and should not be used independently from the FCoE target support. This package contains the AGPL license.

Kernel Media support

The following features are presented as Technology Previews:

- The latest upstream video4linux
- Digital video broadcasting
- Primarily infrared remote control device support
- Various webcam support fixes and improvements

Remote audit logging

The audit package contains the user space utilities for storing and searching the audit records generated by the **`audit`** subsystem in the Linux 2.6 kernel. Within the audispd-plugins subpackage is

a utility that allows for the transmission of audit events to a remote aggregating machine. This remote audit logging application, **audisp-remote**, is considered a Technology Preview in Red Hat Enterprise Linux 6.

Linux (NameSpace) Container [LXC]

Linux containers provide a flexible approach to application runtime containment on bare-metal systems without the need to fully virtualize the workload. Red Hat Enterprise Linux 6.2 provides application level containers to separate and control the application resource usage policies via cgroup and namespaces. This release introduces basic management of container life-cycle by allowing creation, editing and deletion of containers via the **libvirt** API and the **virt-manager** GUI. Linux Containers are a Technology Preview.

Diagnostic pulse for the fence_ipmilan agent, BZ#655764

A diagnostic pulse can now be issued on the IPMI interface using the **`fence_ipmilan`** agent. This new Technology Preview is used to force a kernel dump of a host if the host is configured to do so. Note that this feature is not a substitute for the **`off`** operation in a production cluster.

EDAC driver support, BZ#647700

Red Hat Enterprise Linux 6.2's EDAC driver support for the latest Intel chipset is available as a Technical Preview.

1.7. VIRTUALIZATION

System monitoring via SNMP, BZ#642556

This feature provides KVM support for stable technology that is already used in data center with bare metal systems. SNMP is the standard for monitoring and is extremely well understood as well as computationally efficient. System monitoring via SNMP in Red Hat Enterprise Linux 6.2 allows the KVM hosts to send SNMP traps on events so that hypervisor events can be communicated to the user via standard SNMP protocol. This feature is provided through the addition of a new package: libvirt-snmp. This feature is introduced as a Technology Preview.

Wire speed requirement in KVM network drivers

Virtualization and cloud products that run networking work loads need to run wire speeds. Up until Red Hat Enterprise Linux 6.1, the only way to reach wire speed on a 10 GB Ethernet NIC with a lower CPU utilization was to use PCI device assignment (passthrough), which limits other features like memory overcommit and guest migration

The **macvtap**/**vhost** zero-copy capabilities allows the user to use those features when high performance is required. This feature improves performance for any Red Hat Enterprise Linux 6.x guest in the VEPA use case. This feature is introduced as a Technology Preview.

CHAPTER 2. KNOWN ISSUES

2.1. INSTALLATION

anaconda component, BZ#676025

Users performing an upgrade using the Anaconda's text mode interface who do not have a boot loader already installed on the system, or who have a non-GRUB boot loader, need to select **`Skip Boot Loader Configuration`** during the installation process. Boot loader configuration will need to be completed manually after installation. This problem does not affect users running Anaconda in the graphical mode (graphical mode also includes VNC connectivity mode).

anaconda component

Anaconda fails to install to partitions of size 2.2 TB and larger.

anaconda component

On s390x systems, you cannot use automatic partitioning and encryption. If you want to use storage encryption, you must perform custom partitioning. Do not place the **`/boot`** volume on an encrypted volume.

anaconda component

The order of device names assigned to USB attached storage devices is not guaranteed. Certain USB attached storage devices may take longer to initialize than others, which can result in the device receiving a different name than you expect (for example, **`sdc`** instead of **`sda`**).

During installation, verify the storage device size, name, and type when configuring partitions and file systems.

`kernel` component

Dell systems based on a future Intel processor with graphics acceleration require the selection of the **`install system with basic video driver`** installation option. A future Red Hat Enterprise Linux 6.2.z Extended Update Support update will remove this requirement.

`kernel` component

Recent Red Hat Enterprise Linux 6 releases use a new naming scheme for network interfaces on some machines. As a result, the installer may use different names during an upgrade in certain scenarios (typically **`em1`** is used instead of **`eth0`** on new Dell machines). However, the previously used network interface names are preserved on the system and the upgraded system will still use the previously used interfaces. This is not the case for Yum upgrades.

anaconda component

The **`kdump default on`** feature currently depends on Anaconda to insert the ***`crashkernel=`*** parameter to the kernel parameter list in the boot loader's configuration file.

`firstaidkit` component

The firstaidkit-plugin-grub package has been removed from Red Hat Enterprise Linux 6.2. As a consequence, in rare cases, the system upgrade operation may fail with unresolved dependencies if the plug-in has been installed in a previous version of Red Hat Enterprise Linux. To avoid this problem, the firstaidkit-plugin-grub package should be removed before upgrading the system. However, in most cases, the system upgrade completes as expected.

anaconda component, BZ#623261

In some circumstances, disks that contain a whole disk format (for example, a LVM Physical Volume populating a whole disk) are not cleared correctly using the **clearpart --initlabel** kickstart command. Adding the **--all** switch—as in **clearpart --initlabel --all**—ensures disks are cleared correctly.

squashfs-tools component

During the installation on POWER systems, error messages similar to:

```
attempt to access beyond end of device
loop0: rw=0, want=248626, limit=248624
```

may be returned to **sys.log**. These errors do not prevent installation and only occur during the initial setup. The file system created by the installer will function correctly.

anaconda component

When installing on the IBM System z architecture, if the installation is being performed over SSH, avoid resizing the terminal window containing the SSH session. If the terminal window is resized during the installation, the installer will exit and the installation will terminate.

yaboot component, BZ#613929

The kernel image provided on the CD/DVD is too large for Open Firmware. Consequently, on the POWER architecture, directly booting the kernel image over a network from the CD/DVD is not possible. Instead, use **yaboot** to boot from a network.

anaconda component

The Anaconda partition editing interface includes a button labeled **Resize**. This feature is intended for users wishing to shrink an existing file system and an underlying volume to make room for an installation of a new system. Users performing manual partitioning cannot use the **Resize** button to change sizes of partitions as they create them. If you determine a partition needs to be larger than you initially created it, you must delete the first one in the partitioning editor and create a new one with the larger size.

system-config-kickstart component

Channel IDs (read, write, data) for network devices are required for defining and configuring network devices on IBM S/390 systems. However, **system-config-kickstart**—the graphical user interface for generating a **kickstart** configuration—cannot define channel IDs for a network device. To work around this issue, manually edit the **kickstart** configuration that **system-config-kickstart** generates to include the desired network devices.

dracut component

During FCoE BFS installation, when an Ethernet interface goes offline after discovering the targets, FCoE link will never come up. This is because Anaconda creates an FCoE configuration file under**/etc/fcoe/** using **biosdevname** (new style interface naming scheme) for all the available Ethernet interfaces for FCoE BFS. However, it does not add the ***ifname*** kernel command line for the FCoE interface that stays offline after discovering FCoE targets during installation. Because of this, during subsequent reboots, the system tries to find the old style ethX interface name in the **/etc/fcoe** directory, which does not match with the file created by Anaconda using **biosdevname**. Therefore, due to the missing FCoE configuration file, an FCoE interface is never created on the Ethernet interface.

To avoid this problem, ensure that the Ethernet interface does not go offline during FCoE BFS installation.

If the Ethernet interface does go offline during installation after discovering the targets, add the following parameter to the kernel command line:

```
ifname=<biosdevname_interface_name>:<mac_address>
```

2.2. ENTITLEMENT

subscription manager component

When registering a system with **firstboot**, the *RHN Classic* option is checked by default in the Subscription part.

2.3. DEPLOYMENT

cpuspeed component, BZ#626893

Some HP Proliant servers may report incorrect CPU frequency values in **/proc/cpuinfo** or **/sys/device/system/cpu/*/cpufreq**. This is due to the firmware manipulating the CPU frequency without providing any notification to the operating system. To avoid this ensure that the **HP Power Regulator** option in the BIOS is set to ***OS Control***. An alternative available on more recent systems is to set **Collaborative Power Control** to ***Enabled***.

releng component, BZ#644778

Some packages in the Optional repositories on RHN have multilib file conflicts. Consequently, these packages cannot have both the primary architecture (for example, x86_64) and secondary architecture (for example, i686) copies of the package installed on the same machine simultaneously. To work around this issue, install only one copy of the conflicting package.

releng component

The openmpi-psm and openmpi-psm-devel packages are not provided on architectures other than AMD64 and Intel 64 for Red Hat Enterprise Linux 6.2. If the openmpi-psm.i686 or/and openmpi-psm-devel.i686 packages are installed on a AMD64 or an Intel 64 system, remove these packages before you attempt to update Open MPI.

grub component, BZ#695951

On certain UEFI-based systems, you may need to type **BOOTX64** rather than **bootx64** to boot the installer due to case sensitivity issues.

grub component, BZ#698708

When rebuilding the grub package on the x86_64 architecture, the glibc-static.i686 package must be used. Using the glibc-static.x86_64 package will not meet the build requirements.

parted component

The **parted** utility in Red Hat Enterprise Linux 6 cannot handle Extended Address Volumes (EAV) Direct Access Storage Devices (DASD) that have more than 65535 cylinders. Consequently, EAV DASD drives cannot be partitioned using **parted**, and installation on EAV DASD drives will fail. To

work around this issue, complete the installation on a non EAV DASD drive, then add the EAV device after the installation using the tools provided in the s390-utils package.

`PackageKit` component

If you are being asked repeatedly to enter your root password while using PackageKit to update your system via non-Red Hat repositories, you may be affected by the **PackageKit** issue described in Section 2.11, “Desktop”.

2.4. VIRTUALIZATION

`ovirt-node` component, BZ#747102

Upgrades from Beta to the GA version will result in an incorrect partitioning of the host. The GA version must be installed clean. UEFI machines must be set to legacy boot options for RHEV-H to boot successfully after installation.

`kernel` component

When a system boots from SAN, it starts the **`libvirtd`** service, which enables IP forwarding. The service causes a driver reset on both Ethernet ports which causes a loss of all paths to an OS disk. Under this condition, the system cannot load firmware files from the OS disk to initialize Ethernet ports, eventually never recovers paths to the OS disk, and fails to boot from SAN. To work around this issue add the **`bnx2x.disable_tpa=1`** option to the kernel command line of the GRUB menu, or do not install virtualization related software and manually enable IP forwarding when needed.

`kernel` component

Booting Red Hat Enterprise Linux 6.2 as an HVM guest with more than one vCPU on machines that support SMEP and using Red Hat Enterprise Linux 5.7 and earlier Xen Hypervisors fails. To work around this issue, boot the guest with the **`nosmep`** kernel command line option.

`vdsm` component

If the **`/root/.ssh`** directory is missing from a host when it is added to a Red Hat Enterprise Virtualization Manager data center, the directory is created with a wrong SELinux context, and SSH'ing into the host is denied. To work around this issue, manually create the **`/root/.ssh`** directory with the correct SELinux context:

```
~]# mkdir /root/.ssh
~]# chmod 0700 /root/.ssh
~]# restorecon /root/.ssh
```

`vdsm` component

VDSM now configures **libvirt** so that connection to its local read-write UNIX domain socket is password-protected by SASL. The intention is to protect virtual machines from human errors of local host administrators. All operations that may change the state of virtual machines on a Red Hat Enterprise Virtualization-controlled host must be performed from Red Hat Enterprise Virtualization Manager.

`libvirt` component

In earlier versions of Red Hat Enterprise Linux, **libvirt** permitted PCI devices to be insecurely assigned to guests. In Red Hat Enterprise Linux 6, assignment of insecure devices is disabled by default by **libvirt**. However, this may cause assignment of previously working devices to start failing.

To enable the old, insecure setting, edit the **/etc/libvirt/qemu.conf** file, set the ***relaxed_acs_check = 1*** parameter, and restart **libvirtd** (**service libvirtd restart**). Note that this action will re-open possible security issues.

virtio-win component, BZ#615928

The balloon service on Windows 7 guests can only be started by the Administrator user.

libvirt component, BZ#622649

libvirt uses transient **iptables** rules for managing NAT or bridging to virtual machine guests. Any external command that reloads the **iptables** state (such as running **system-config-firewall**) will overwrite the entries needed by **libvirt**. Consequently, after running any command or tool that changes the state of **iptables**, guests may lose access the network. To work around this issue, use the **service libvirt reload** command to restore **libvirt**'s additional **iptables** rules.

virtio-win component, BZ#612801

A Windows virtual machine must be restarted after the installation of the kernel Windows driver framework. If the virtual machine is not restarted, it may crash when a memory balloon operation is performed.

qemu-kvm component, BZ#720597

Installation of Windows 7 Ultimate x86 (32-bit) Service Pack 1 on a guest with more than 4GB of RAM and more than one CPU from a DVD medium often crashes during the final steps of the installation process due to a system hang. To work around this issue, use the Windows Update utility to install the Service Pack.

qemu-kvm component, BZ#612788

A dual function Intel 82576 Gigabit Ethernet Controller interface (codename: Kawela, PCI Vendor/Device ID: 8086:10c9) cannot have both physical functions (PF's) device-assigned to a Windows 2008 guest. Either physical function can be device assigned to a Windows 2008 guest (PCI function 0 or function 1), but not both.

virt-v2v component

In Red Hat Enterprise Linux 6.2, the default **virt-v2v** configuration is split into two files: **/etc/virt-v2v.conf** and **/var/lib/virt-v2v/virt-v2v.db**. The former now contains only local customizations, whereas the latter contains generic configuration which is not intended to be customized. Prior to Red Hat Enterprise Linux 6.2, **virt-v2v**'s **-f** flag defaulted to **/etc/virt-v2v.conf**. In Red Hat Enterprise Linux 6.2, it now defaults to both**/etc/virt-v2v.conf** and **/var/lib/virt-v2v/virt-v2v.db**. Data from both of these files is required during conversion.

This change has no impact for most users. If a machine is upgraded from Red Hat Enterprise Linux 6.1 to Red Hat Enterprise Linux 6.2, the existing combined **/etc/virt-v2v.conf** will not be updated. If a user explicitly specifies **-f /etc/virt-v2v.conf** on the command line, the behavior will be identical to the one prior to update. If the user does not specify the **-f** command line option, the configuration will use both **/etc/virt-v2v.conf** and **/var/lib/virt-v2v/virt-v2v.db**, with the former taking precedence.

However, a freshly-installed Red Hat Enterprise Linux 6.2 machine with a default configuration no longer has all required data in **/etc/virt-v2v.conf**. If the user explicitly specifies **-f /etc/virt-v2v.conf** on the command line, **virt-v2v** will not be able to enable **virtio** support for any guests.

To work around this issue, do use the **-f** command line option, as this defaults to using both configuration files. If the **-f** command line option is used, it must be specified twice: first for **/etc/virt-v2v.conf** and second for **/var/lib/virt-v2v/virt-v2v.conf**.

If the **virt-v2v** command line cannot be altered, the **/etc/virt-v2v.conf** file must contain a combined configuration file. This can be copied from a Red Hat Enterprise Linux 6.1 system, or created by copying all configuration elements from **/var/lib/virt-v2v/virt-v2v.db** to **/etc/virt-v2v.conf**.

virt-v2v component, BZ#618091

The **virt-v2v** utility is able to convert guests running on an ESX server. However, if an ESX guest has a disk with a snapshot, the snapshot must be on the same datastore as the underlying disk storage. If the snapshot and the underlying storage are on different datastores, **virt-v2v** will report a 404 error while trying to retrieve the storage.

virt-v2v component, BZ#678232

The VMware Tools application on Microsoft Windows is unable to disable itself when it detects that it is no longer running on a VMware platform. Consequently, converting a Microsoft Windows guest from VMware ESX, which has VMware Tools installed, will result in errors. These errors usually manifest as error messages on start-up, and a "Stop Error" (also known as a BSOD) when shutting down the guest. To work around this issue, uninstall VMware Tools on Microsoft Windows guests prior to conversion.

spice-client component

Sound recording only works when there is no application accessing the recording device at the client start-up.

2.5. STORAGE AND FILE SYSTEMS

device-mapper-multipath component

Multipath's **queue_without_daemon yes** default option queues I/O even though all iSCSI links have been disconnected when the system is shut down, which causes LVM to become unresponsive when scanning all block devices. As a result, the system cannot be shut down. To work around this issue, add the following line into the **defaults** section of **/etc/multipath.conf**:

```
queue_without_daemon no
```

initscripts component

If the **/etc/fstab** file contains an NFS mount entry that has the file system check (**fsck**) enabled, the **netfs** service responsible for mounting and unmounting NFS file systems initializes the file system check. Because NFS is not a block-level file system, this operation fails, and subsequently also fails the system boot itself. To work around this problem, disable the file system check by setting the sixth vaule for NFS mount entries to **0**.

iscsi-initiator-utils component, BZ#739843

iSCSI discovery via a TOE (TCP Offload Engine) interface fails when the **iscsiadm -m iface** has never been executed. This is due to the **iscsiadm -m discovery** command not checking interface settings while the **iscsiadm -m iface** does. To work around this issue, run the **iscsiadm -m**

iface command at least once after installing the iscsi-initiatio-utils package. Once the interface setting is updated, discoveries are performed with no errors.

vdsm component

Attempting to create/extend a storage domain on/with a device that exposes a block size different than 512 bytes such create/extend request to fail. To work around this issue, the storage must be configured to expose a block size of 512 bytes.

kernel component, BZ#606260

The NFSv4 server in Red Hat Enterprise Linux 6 currently allows clients to mount using UDP and advertises NFSv4 over UDP with **rpcbind**. However, this configuration is not supported by Red Hat and violates the RFC 3530 standard.

lvm2 component

The **dracut** utility currently only supports one FiberChannel over Ethernet (FCoE) connection to be used to boot from the root device. Consequently, booting from a root device that spans multiple FCoE devices (for example, using RAID, LVM or similar techniques) is not possible.

lvm2 component

The **pvmove** command cannot currently be used to move mirror devices. However, it is possible to move mirror devices by issuing a sequence of two commands. For mirror images, add a new image on the destination PV and then remove the mirror image on the source PV:

```
~]$ lvconvert -m +1 <vg/lv> <new PV>
~]$ lvconvert -m -1 <vg/lv> <old PV>
```

Mirror logs can be handled in a similar fashion:

```
~]$ lvconvert --mirrorlog core <vg/lv>
~]$ lvconvert --mirrorlog disk <vg/lv> <new PV>
```

or

```
~]$ lvconvert --mirrorlog mirrored <vg/lv> <new PV>
~]$ lvconvert --mirrorlog disk <vg/lv> <old PV>
```

2.6. NETWORKING

NetworkManager component

To ensure that RFC3442-standard classless static routes provided by a DHCP server are processed correctly when using NetworkManager, the following lines should be placed into the **/etc/dhclient.conf** file or, if using per-interface DHCP options, the **/etc/dhclient-<ifname>.conf** file:

```
option rfc3442-classless-static-routes code 121 = array of unsigned
integer 8;
option ms-classless-static-routes code 249 = array of unsigned integer
8;
also request rfc3442-classless-static-routes;
also request ms-classless-static-routes;
```

The above lines will ensure that RFC3442 classless static routes are requested from the DHCP server, and that they are properly processed by NetworkManager.

`iprutils` component

Users of the IBM PCI-E Gen2 6GB SAS RADI adapter (FC 5913) in Red Hat Enterprise Linux 6.2 may encounter the following issues:

- Updating firmware on a storage drawer that is connected to the adapter mentioned above using the **`iprconfig`** command fails.
- Attempting to change the asymmetric access for an array results in a failure. Additionally, not specifying asymmetric access as an option to the **`iprconfig`** command results in a failure as well.

2.7. CLUSTERING

`corosync` component, BZ#722469

A double ring failure results in the spinning of the corosync process. Also, because DLM relies on SCTP, which is non-functional, many features of the cluster software that rely on DLM do not work properly.

`luci` component, BZ#615898

`luci` will not function with Red Hat Enterprise Linux 5 clusters unless each cluster node has **`ricci`** version 0.12.2-14

2.8. AUTHENTICATION

Identity Management component

When transitioning to a fully supported Identity Management version in Red Hat Enterprise Linux 6.2, uninstall any previous beta version of Identity Management or Technology Preview parts of Red Hat Enterprise Identity (IPA) available in the Red Hat Enterprise Linux 6.1 Technology Preview and install Identity Management again.

Identity Management component

When an Identity Management server is installed with a custom hostname that is not resolvable, the **`ipa-server-install`** command should add a record to the static hostname lookup table in **`/etc/hosts`** and enable further configuration of Identity Management integrated services. However, a record is not added to **`/etc/hosts`** when an IP address is passed as an CLI option and not interactively. Consequently, Identity Management installation fails because integrated services that are being configured expect the Identity Management server hostname to be resolvable. To work around this issue, complete one of the following:

- Run the **`ipa-server-install`** without the **`--ip-address`** option and pass the IP address interactively.
- Add a record to **`/etc/hosts`** before the installation is started. The record should contain the Identity Management server IP address and its full hostname (the **`hosts(5)`** man page specifies the record format).

As a result, the Identity Management server can be installed with a custom hostname that is not resolvable.

sssd component, BZ#750922

Upgrading SSSD from the version provided in Red Hat Enterprise Linux 6.1 to the version shipped with Red Hat Enterprise Linux 6.2 may fail due to a bug in the dependent library **libldb**. This failure occurs when the SSSD cache contains internal entries whose distinguished name contains the `\,` character sequence. The most likely example of this is for an invalid ***memberUID*** entry to appear in an LDAP group of the form:

```
memberUID: user1,user2
```

memberUID is a multi-valued attribute and should not have multiple users in the same attribute.

If the upgrade issue occurs, identifiable by the following debug log message:

```
(Wed Nov  2 15:18:21 2011) [sssd] [ldb] (0): A transaction is still
active in
ldb context [0xaa0460] on /var/lib/sss/db/cache_<DOMAIN>.ldb
```

remove the **/var/lib/sss/db/cache_<DOMAIN>.ldb** file and restart SSSD.

WARNING

Removing the **/var/lib/sss/db/cache_<DOMAIN>.ldb** file purges the cache of all entries (including cached credentials).

sssd component, BZ#751314

When a group contains certain incorrect multi-valued ***memberUID*** values, SSSD fails to sanitize the values properly. The ***memberUID*** value should only contain one username. As a result, SSSD creates incorrect users, using the broken ***memberUID*** values as their usernames. This, for example, causes problems during cache indexing.

Identity Management component, BZ#750596

Two Identity Management servers, both with a CA (Certificate Authority) installed, use two replication replication agreements. One is for user, group, host, and other related data. Another replication agreement is established between the CA instances installed on the servers. If the CA replication agreement is broken, the Identity Management data is still shared between the two servers, however, because there is no replication agreement between the two CAs, issuing a certificate on one server will cause the other server to not recognize that certificate, and vice versa.

Identity Management component

The Identity Management (ipa) package cannot be build with a **6ComputeNode** subscription.

Identity Management component

On the configuration page of the Identity Management WebUI, if the **User** search field is left blank, and the **search** button is clicked, an internal error is returned.

sssd component, BZ#741264

Active Directory performs certain LDAP referral-chasing that is incompatible with the referral mechanism included in the **openldap** libraries. Notably, Active Directory sometimes attempts to return a referral on an LDAP bind attempt, which used to cause a hang, and is now denied by the **openldap** libraries. As a result, SSSD may suffer from performance issues and occasional failures resulting in missing information.

To work around this issue, disable referral-chasing by setting the following parameter in the **[domain/DOMAINNAME]** section of the **/etc/sssd/sssd.conf** file:

```
ldap_referrals = false
```

2.9. DEVICES

kernel component

The Red Hat Enterprise Linux 6.2 Emulex FC (lpfc) driver does not support firmware downloads for LPe1600x 16 Gbit/s Fibre Channel adapters. Please consult your OEM for instructions on how to download new firmware on these Fibre Channel adapters.

kernel component

iSCSI and FCoE boot support on Broadcom devices is not included in Red Hat Enterprise Linux 6.2. These two new features, which have been added to the **bnx2i** and **bnx2fc** Broadcom drivers in Red Hat Enterprise Linux 6.2, remain a Technology Preview until further notice.

kexec-tools component

Starting with Red Hat Enterprise Linux 6.0 and later, kexec kdump supports dumping core to the Brtfs file system. However, note that because the **findfs** utility in **busybox** does not support Btrfs yet, ***UUID/LABEL*** resolving is not functional. Avoid using the ***UUID/LABEL*** syntax when dumping core to Btrfs file systems.

kexec-tools component, BZ#600575

The persistent naming of devices that are dynamically discovered in a system is a large problem that exists both in and outside of kdump. Normally, devices are detected in the same order, which leads to consistent naming. In cases where devices are not detected in the same order, device abstraction layers (for example, LVM) essentially resolve the issue, through the use of metadata stored on the devices to create consistency. In the rare cases where no such abstraction layer is in use, and renaming devices causes issues with kdump, it is recommended that devices be referred to by disk label or UUID in **kdump.conf**.

trace-cmd component

The **trace-cmd** service does start on 64-bit PowerPC and IBM System z systems because the **sys_enter** and **sys_exit** events do not get enabled on the aforementioned systems.

trace-cmd component

trace-cmd's subcommand, **report**, does not work on IBM System z systems. This is due to the fact that the ***CONFIG_FTRACE_SYSCALLS*** parameter is not set on IBM System z systems.

`tuned` component

Red Hat Enterprise Linux 6.1 and later enter processor power-saving states more aggressively. This may result in a small performance penalty on certain workloads. This functionality may be disabled at boot time by passing the ***`intel_idle.max_cstate=0`*** parameter, or at run time by using the **cpu_dma_latency pm_qos** interface.

`libfprint` component

Red Hat Enterprise Linux 6 only has support for the first revision of the UPEK Touchstrip fingerprint reader (USB ID 147e:2016). Attempting to use a second revision device may cause the fingerprint reader daemon to crash. The following command returns the version of the device being used in an individual machine:

```
~]$ lsusb -v -d 147e:2016 | grep bcdDevice
```

`kernel` component

The Emulex Fibre Channel/Fibre Channel-over-Ethernet (FCoE) driver in Red Hat Enterprise Linux 6 does not support DH-CHAP authentication. DH-CHAP authentication provides secure access between hosts and mass storage in Fibre-Channel and FCoE SANs in compliance with the FC-SP specification. Note, however that the Emulex driver (**`lpfc`**) does support DH-CHAP authentication on Red Hat Enterprise Linux 5, from version 5.4. Future Red Hat Enterprise Linux 6 releases may include DH-CHAP authentication.

`kernel` component

The recommended minimum HBA firmware revision for use with the **`mpt2sas`** driver is "Phase 5 firmware" (that is, with version number in the form **`05.xx.xx.xx`**). Note that following this recommendation is especially important on complex SAS configurations involving multiple SAS expanders.

2.10. KERNEL

`kernel` component

When booted off a **`qla4xxx`** device, upgrading from Red Hat Enterprise Linux 6.1 to Red Hat Enterprise Linux 6.2 will cause the system to fail to boot up with the new kernel. There are various ways to work around this issue:

1. You have upgraded to Red Hat Enterprise Linux 6.2 and want the **`qla4xxx`** device firmware to manage discovering and logging in to iSCSI targets.
    1. Boot up the system with the Red Hat Enterprise Linux 6.1 kernel.
    2. Disable SysfsBoot for the **`qla4xxx`** device:

        ```
        ~]# echo "options qla4xxx ql4xdisablesysfsboot=1" >>
        /etc/modprobe.d/qla4xxx.conf
        ```

    3. Rebuild initramfs for the Red Hat Enterprise Linux 6.2 kernel by re-installing the kernel:

        ```
        ~]# yum -y reinstall kernel
        ```

2. You have not upgraded to Red Hat Enterprise Linux 6.2 and want the **qla4xxx** device firmware to manage discovering and logging in to iSCSI targets.

    1. Boot up the system with the Red Hat Enterprise Linux 6.1 kernel.

    2. Disable SysfsBoot for the **qla4xxx** device:

    ```
    ~]# echo "options qla4xxx ql4xdisablesysfsboot=1" >>
    /etc/modprobe.d/qla4xxx.conf
    ```

    3. Proceed with the upgrade to Red Hat Enterprise Linux 6.2.

3. You have upgraded to Red Hat Enterprise Linux 6.2 and want to use **open-iscsi** to manage the **qla4xxx** discovery and login process.

    1. Boot up the system with the Red Hat Enterprise Linux 6.1 kernel.

    2. Install the iscsi-initiator-utils and dracut-network packages:

    ```
    ~]# yum install -y dracut-network iscsi-initiator-utils
    ```

    3. Rebuild initramfs for the Red Hat Enterprise Linux 6.2 kernel by re-installing the kernel:

    ```
    ~]# yum -y reinstall kernel
    ```

    4. Add the **iscsi_firmware** kernel option into GRUB's configuration: **/boot/grub/menu.lst** (for LILO, the Linux Loader, modify the **/etc/lilo.conf** file).

4. You have not upgraded to Red Hat Enterprise Linux 6.2 and want to use **open-iscsi** to manage the **qla4xxx** discovery and login process.

    1. Install the iscsi-initiator-utils and dracut-network packages:

    ```
    ~]# yum install -y dracut-network iscsi-initiator-utils
    ```

    2. Proceed with the upgrade to Red Hat Enterprise Linux 6.2.

    3. Add the **iscsi_firmware** kernel option into GRUB's configuration: **/boot/grub/menu.lst** (for LILO, the Linux Loader, modify the **/etc/lilo.conf** file).

kernel component, BZ#679262

In Red Hat Enterprise Linux 6.2, due to security concerns, addresses in **/proc/kallsyms** and **/proc/modules** show all zeros when accessed by a non-root user.

kernel component

Red Hat Enterprise Linux 6.1 PCI-Express Adapters may fail to configure on October 2011 GA IBM Power 7 systems. For more information, refer to https://access.redhat.com/site/solutions/66231.

kernel component

Superfluous information is displayed on the console due to a correctable machine check error

occurring. This information can be safely ignored by the user. Machine check error reporting can be disabled by using the **nomce** kernel boot option, which disables machine check error reporting, or the **mce=ignore_ce** kernel boot option, which disables correctable machine check error reporting.

kernel component

The order in which PCI devices are scanned may change from one major Red Hat Enterprise Linux release to another. This may result in device names changing, for example, when upgrading from Red Hat Enterprise Linux 5 to 6. You must confirm that a device you refer to during installation, is the intended device.

One way to assure the correctness of device names is to, in some configurations, determine the mapping from the controller name to the controller's PCI address in the older release, and then compare this to the mapping in the newer release, to ensure that the device name is as expected.

The following is an example from /var/log/messages:

```
kernel: cciss0: <0x3230> at PCI 0000:1f:00.0 IRQ 71 using DAC
…
kernel: cciss1: <0x3230> at PCI 0000:02:00.0 IRQ 75 using DAC
```

If the device name is incorrect, add the ***pci=bfsort*** parameter to the kernel command line, and check again.

kernel component

Enabling CHAP (Challenge-Handshake Authentication Protocol) on an iSCSI target for the **be2iscsi** driver results in kernel panic. To work around this issue, disable CHAP on the iSCSI target.

kernel component

Newer VPD (Vital Product Data) blocks can exceed the size the **tg3** driver normally handles. As a result, some of the routines that operate on the VPD blocks may fail. For example, the **nvram** test fails when running the **ethtool -t** command on BCM5719 and BCM5720 Ethernet Controllers.

kernel component

Running the **ethtool -t** command on BCM5720 Ethernet controllers causes a loopback test failure because the **tg3** driver does not wait long enough for a link.

kernel component

The **tg3** driver in Red Hat Enterprise Linux 6.2 does not include support for Jumbo frames and TSO (TCP Segmentation Offloading) on BCM5719 Ethernet controllers. As a result, the following error message is returned when attempting to configure, for example, Jumbo frames:

```
SIOCSIFMTU: Invalid argument
```

kernel component

The default interrupt configuration for the Emulex LPFC FC/FCoE driver has changed from INT-X to MSI-X. This is reflected by the ***lpfc_use_msi*** module parameter (in **/sys/class/scsi_host/host#/lpfc_use_msi**) being set to **2** by default, instead of the previous **0**.

Two issues provide motivation for this change: SR-IOV capability only works with the MSI-X interrupt mode, and certain recent platforms only support MSI or MSI-X.

However, the change to the LPFC default interrupt mode can bring out host problems where MSI/MSI-X support is not fully functional. Other host problems can exist when running in the INT-X mode.

If any of the following symptoms occur after upgrading to, or installing Red Hat Enterprise Linux 6.2 with an Emulex LPFC adapter in the system, change the value of the **lpfc** module parameter, ***lpfc_use_msi***, to **0**:

- The initialization or attachment of the **lpfc** adapter may fail with mailbox errors. As a result, the **lpfc** adapter is not configured on the system. The following message appear in **/var/log/messages**:

```
lpfc 0000:04:08.0: 0:0:0443 Adapter failed to set maximum DMA
length mbxStatus x0
lpfc 0000:04:08.0: 0:0446 Adapter failed to init (255), mbxCmd x9
CFG_RING, mbxStatus x0, ring 0
lpfc 0000:04:08.0: 0:1477 Failed to set up hba
ACPI: PCI interrupt for device 0000:04:08.0 disabled
```

- While the **lpfc** adapter is operating, it may fail with mailbox errors, resulting in the inability to access certain devices. The following message appear in **/var/log/messages**:

```
lpfc 0000:0d:00.0: 0:0310 Mailbox command x5 timeout Data: x0 x700
xffff81039ddd0a00
lpfc 0000:0d:00.0: 0:0345 Resetting board due to mailbox timeout
lpfc 0000:0d:00.0: 0:(0):2530 Mailbox command x23 cannot issue
Data: xd00 x2
```

- Performing a warm reboot causes any subsequent boots to halt or stop because the BIOS is detecting the **lpfc** adapter. The system BIOS logs the following messages:

```
Installing Emulex BIOS ......
Bringing the Link up, Please wait...
Bringing the Link up, Please wait...
```

kernel component

The minimum firmware version for NIC adapters managed by **netxen_nic** is 4.0.550. This includes the boot firmware which is flashed in option ROM on the adapter itself.

kernel component

The kdump kernel occasionally panics on a DELL PowerEdge R810 system with the i686 architecture.

kernel component

Running the LTP (Linux Testing Project) cgroup test suite on certain AMD systems causes NMI Watchdog to detect a hard LOCKUP and cause kernel panic.

kernel component, BZ#683012

High stress on 64-bit IBM POWER series machines prevents kdump from successfully capturing the **vmcore**. As a result, the second kernel is not loaded, and the system becomes unresponsive.

kernel component

Loading and unloading **edac** modules in a loop on certain HP systems may cause kernel panic.

kernel component

If the storage driver is loaded before **multipathd** is started, I/O errors occur. To work around this issue, use one of the following kernel command line parameters which are consumed by **dracut**:

```
rdloaddriver=scsi_dh_emc
```

or

```
rdloaddriver=scsi_dh_rdac
```

or

```
rdloaddriver=scsi_dh_emc,scsi_dh_rdac
```

The above command line parameters will cause the **scsi_dh** module to load before **multipath** is started.

kernel component

Triggering kdump to capture a **vmcore** through the network using the Intel 82575EB ethernet device in a 32 bit environment causes the networking driver to not function properly in the kdump kernel, and prevent the **vmcore** from being captured.

kernel component, BZ#701857

Attempting to hibernate certain laptops, including Lenovo ThinkPad T400 and Lenovo ThinkPad X200, can cause kernel panic.

kernel component

On a system configured with an HP Smart Array controller, during the kdump process, the capturing kernel can become unresponsive and the following error message is logged:

```
NMI: IOCK error (debug interrupt?)
```

As a workaround, the system can be configured by blacklisting the **hpsa** module in a configuration file such as **/etc/modules.d/blacklist.conf**, and specifying the **disk_timeout** option so that saving the **vmcore** over the network is possible.

kernel component

Memory Type Range Register (MTRR) setup on some hyperthreaded machines may be incorrect following a suspend/resume cycle. This can cause graphics performance (specifically, scrolling) to slow considerably after a suspend/resume cycle.

To work around this issue, disable and then re-enable the hyperthreaded sibling CPUs around suspend/resume, for example:

-

```
#!/bin/sh
# Disable hyper-threading processor cores on suspend and hibernate, re-
enable
# on resume.
# This file goes into /etc/pm/sleep.d/

case $1 in
        hibernate|suspend)
                echo 0 > /sys/devices/system/cpu/cpu1/online
                echo 0 > /sys/devices/system/cpu/cpu3/online
                ;;

        thaw|resume)
                echo 1 > /sys/devices/system/cpu/cpu1/online
                echo 1 > /sys/devices/system/cpu/cpu3/online
                ;;
esac
```

kernel component

In Red Hat Enterprise Linux 6.2, **nmi_watchdog** registers with the **perf** subsystem. Consequently, during boot, the **perf** subsystem grabs control of the performance counter registers, blocking OProfile from working. To resolve this, either boot with the **nmi_watchdog=0** kernel parameter set, or run the following command to disable it at run time:

```
echo 0 > /proc/sys/kernel/nmi_watchdog
```

To re-enable **nmi-watchdog**, use the following command

```
echo 1 > /proc/sys/kernel/nmi_watchdog
```

kernel component, BZ#603911

Due to the way **ftrace** works when modifying the code during start-up, the NMI watchdog causes too much noise and **ftrace** can not find a quiet period to instrument the code. Consequently, machines with more than 512 CPUs will encounter issues with the NMI watchdog. Such issues will return error messages similar to **BUG: NMI Watchdog detected LOCKUP** and have either **ftrace_modify_code** or **ipi_handler** in the backtrace. To work around this issue, disable NMI watchdog by setting the **nmi_watchdog=0** kernel parameter, or using the following command at run time:

```
echo 0 > /proc/sys/kernel/nmi_watchdog
```

kernel component

On 64-bit POWER systems the EHEA NIC driver will fail when attempting to dump a **vmcore** via NFS. To work around this issue, utilize other kdump facilities, for example dumping to the local file system, or dumping over SSH.

kernel component, BZ#587909

A BIOS emulated floppy disk might cause the installation or kernel boot process to hang. To avoid this, disable emulated floppy disk support in the BIOS.

kernel component

The preferred method to enable nmi_watchdog on 32-bit x86 systems is to use either ***nmi_watchdog=2*** or ***nmi_watchdog=lapic*** parameters. The parameter ***nmi_watchdog=1*** is not supported.

kernel component

The kernel parameter, **pci=noioapicquirk**, is required when installing the 32-bit variant of Red Hat Enterprise Linux 6 on HP xw9300 workstations. Note that the parameter change is not required when installing the 64-bit variant.

2.11. DESKTOP

PackageKit component

Installing or updating packages signed with a GPG key not known or accessible to the system may throw **PackageKit** in a loop of password dialogues, repeatedly asking the user to confirm the installation of these packages from an untrusted source.

This issue may occur if additional third party repositories are configured on the system for which the GPG public key is not imported into the RPM database, nor specified in the respective Yum repository configuration. Official Red Hat Enterprise Linux repositories and packages should not be affected by this issue.

To work around this issue, import the respective GPG public key into the RPM database by executing the following command as root:

```
~]# rpm --import <file_containing_the_public_key>
```

gnome-power-manager component, BZ#748704

After resuming the system or re-enabling the display, an icon may appear in the notification area with a tooltip that reads:

```
Session active, not inhibited, screen idle. If you see this test, your
display server is broken and you should notify your distributor. Please
see http://blogs.gnome.org/hughsie/2009/08/17/gnome-power-manager-and-
blanking-removal-of-bodges/ for more information.
```

This error message is incorrect, has no effect on the system, and can be safely ignored.

acroread component

Running a AMD64 system without the sssd-client.i686 package installed, which uses SSSD for getting information about users, causes **acroread** to fail to start. To work around this issue, manually install the sssd-client.i686 package.

kernel component, BZ#681257

With newer kernels, such as the kernel shipped in Red Hat Enterprise Linux 6.1, Nouveau has corrected the Transition Minimized Differential Signaling (TMDS) bandwidth limits for pre-G80 nVidia chipsets. Consequently, the resolution auto-detected by X for some monitors may differ from that used in Red Hat Enterprise Linux 6.0.

fprintd component

When enabled, fingerprint authentication is the default authentication method to unlock a workstation, even if the fingerprint reader device is not accessible. However, after a 30 second wait, password authentication will become available.

`evolution` component

Evolution's IMAP backend only refreshes folder contents under the following circumstances: when the user switches into or out of a folder, when the auto-refresh period expires, or when the user manually refreshes a folder (that is, using the menu item **Folder** → **Refresh**). Consequently, when replying to a message in the Sent folder, the new message does not immediately appear in the Sent folder. To see the message, force a refresh using one of the methods describe above.

`anaconda` component

The clock applet in the GNOME panel has a default location of Boston, USA. Additional locations are added via the applet's preferences dialog. Additionally, to change the default location, left-click the applet, hover over the desired location in the **`Locations`** section, and click the **`Set...`** button that appears.

`xorg-x11-server` component, BZ#623169

In some multi-monitor configurations (for example, dual monitors with both rotated), the cursor confinement code produces incorrect results. For example, the cursor may be permitted to disappear off the screen when it should not, or be prevented from entering some areas where it should be allowed to go. Currently, the only workaround for this issue is to disable monitor rotation.

CHAPTER 3. NEW PACKAGES

3.1. RHEA-2011:1627 — NEW PACKAGES: BTPARSER

New btparser packages are now available for Red Hat Enterprise Linux 6.

The btparser is a backtrace parser and analyzer library, which works with backtraces produced by the GNU Project Debugger. It can parse a text file with a backtrace to a tree of C structures, allowing to analyze the threads and frames of the backtrace and process them.

This enhancement update adds the btparser package to Red Hat Enterprise Linux 6. (BZ#708038)

All users who require btparser are advised to install this new package.

3.2. RHEA-2011:1729 — NEW PACKAGE: FCOE-TARGET-UTILS

A new fcoe-target-utils package is now available as a Technology Preview for Red Hat Enterprise Linux 6.

The fcoe-target-utils package is a command line interface for configuring FCoE LUNs (Fibre Channel over Ethernet Logical Unit Numbers) and backstores.

This enhancement update adds a new fcoe-target-utils package to Red Hat Enterprise Linux 6 as a Technology Preview. (BZ#724035)

More information about Red Hat Technology Previews is available here:

https://access.redhat.com/support/offerings/techpreview/

All users who want to use the fcoe-target-utils Technology Preview should install this newly-released package, which adds this enhancement.

3.3. RHEA-2011:1653 — NEW PACKAGE: LIBUNISTRING

A new libunistring package is now available for Red Hat Enterprise Linux 6.

This portable C library implements the UTF-8, UTF-16 and UTF-32 Unicode string types, together with functions for character processing (names, classifications, and properties) and functions for string processing (iteration, formatted output, width, word breaks, line breaks, normalization, case folding, and regular expressions).

This enhancement update adds the libunistring package to Red Hat Enterprise Linux 6. The libunistring package has been added as a dependency for the System Security Services Daemon (SSSD) in order to process internationalized HBAC rules on FreeIPA servers. (BZ#726463)

All users who require libunistring should install this new package.

3.4. RHEA-2011:1636 — NEW PACKAGE: LIBVIRT-QMF

A new libvirt-qmf package is now available for Red Hat Enterprise Linux 6.

The libvirt-qmf package contains a daemon to allow remote control of the libvirt API through the Qpid Management Framework (QMF).

Enhancement

BZ#688194

With this update, the libvirt-qmf package obsoletes the libvirt-qpid package, which provided similar functionality. The new package uses the matahari library to provide an interface consistent with that of other Matahari agents.

Note: After installation, it is advisable to convert existing QMF consoles, that previously connected to libvirt-qpid, to use libvirt-qmf as their interface. Also, when creating a new QMF console, it is recommended to use libvirt-qmf to communicate with libvirt.

All users requiring libvirt-qmf are advised to install this new package, which adds this enhancement.

3.5. RHEA-2011:1609 — NEW PACKAGE: LIBVIRT-SNMP

A new libvirt-snmp package is now available for Red Hat Enterprise Linux 6.

The new package libvirt-snmp allows to control and monitor libvirt virtualization management tool by the way of the SNMP protocol. SNMP is an Internet-standard protocol for managing devices on IP networks, its modular structure allows it to be used in new fields and this new package allow virtualization management by bridging the SNMP protocol and the libvirt API.

This enhancement update adds the libvirt-snmp package to Red Hat Enterprise Linux 6. (BZ#642556, BZ#706114)

All users who require libvert-snmp are advised to install this new package.

3.6. RHEA-2011:1714 — NEW PACKAGES: MESA-LIBGLW

New mesa-libGLw packages are now available for Red Hat Enterprise Linux 6.

The mesa-libGLw packages provide an Xt/Motif OpenGL Drawing Area Widget.

This enhancement update adds the esa-libGLw package to Red Hat Enterprise Linux 6. (BZ#729243)

All users who require mesa-libGLw are advised to install these new packages.

3.7. RHBA-2011:1628 — NEW PACKAGE: OPENSLP

A new openslp package is now available for Red Hat Enterprise Linux 6.

OpenSLP is an open source implementation of the Service Location Protocol (SLP) which is an Internet Engineering Task Force (IETF) standards track protocol and provides a framework to allow networking applications to discover the existence, location, and configuration of networked services in enterprise networks.

This enhancement update adds the openslp package to Red Hat Enterprise Linux 6. (BZ#518286)

All users who require OpenSLP are advised to install this new package.

3.8. RHEA-2011:1545 — NEW PACKAGE: PASSSYNC

A new passsync package is now available for Red Hat Enterprise Identity Replication.

PassSync is a Windows service that runs on every domain controller. This intercepts clear text password updates and sends them to the directory server running on Red Hat Enterprise Linux.

PassSync works together with the Windows Synchronization (WinSync) feature of the directory server to keep passwords synchronized between Active Directory (AD) and the directory server running on Red Hat Enterprise Linux.

This enhancement update adds the passsync package to Red Hat Enterprise Identity Replication which is an add-on for Red Hat Enterprise Linux 6. (BZ#690622)

Users who require password synchronization together with WinSync are advised to install this new package.

3.9. RHEA-2011:1731 — NEW PACKAGE: PERL-TEST-INTER

A new perl-Test-Inter package is now available for Red Hat Enterprise Linux 6.

The Test::Inter module provides a framework for writing interactive test scripts in Perl. It is inspired by the Test::More framework.

This enhancement update adds the perl-Test-Inter package to Red Hat Enterprise Linux 6. (BZ#705752)

All users who require perl-Test-Inter should install this new package.

3.10. RHEA-2011:1725 — NEW PACKAGE: PYTHON-CONFIGSHELL

A new python-configshell package is now available for Red Hat Enterprise Linux 6.

The python-configshell package provides a library for implementing configuration command line interfaces for the Python programming environment.

This enhancement update adds the python-configshell package to Red Hat Enterprise Linux 6 as part of the Technology Preview of Fibre Channel over Ethernet (FCoE) target mode. (BZ#726774)

IMPORTANT

This package is provided as a dependency of the fcoe-target-utils package. It is recommended to install it only as a prerequisite for running fcoe-target-utils, and not to use it independently.

All users who want to use the Technology Preview of Fibre Channel over Ethernet target mode should install this newly-released package, which adds this enhancement.

3.11. RHEA-2011:1724 — NEW PACKAGE: PYTHON-IPADDR

A new python-ipaddr package is now available for Red Hat Enterprise Linux 6.

The python-ipaddr package is a library for working with IPv4 and IPv6 addresses for the Python programming environment.

This enhancement update adds the python-ipaddr package to Red Hat Enterprise Linux 6. (BZ#726773)

This is being added as part of the Tech Preview of FCoE (Fibre Channel over Ethernet) target mode, as a dependency of fcoe-target-utils. It is recommended to install this library only as a prerequisite for running fcoe-target-utils, and it should not be used independently.

3.12. RHEA-2011:1728 — NEW PACKAGE: PYTHON-RTSLIB

A new python-rtslib package is now available for Red Hat Enterprise Linux 6.

The python-rtslib package provides a library for interacting with storage target-related interfaces for the Python programming environment.

This enhancement update adds the python-rtslib package to Red Hat Enterprise Linux 6 as part of the Technology Preview of Fibre Channel over Ethernet (FCoE) target mode. (BZ#726778)

IMPORTANT

This package is provided as a dependency of the fcoe-target-utils package. It is recommended to install it only as a prerequisite for running fcoe-target-utils, and not to use it independently.

All users who want to use the Technology Preview of Fibre Channel over Ethernet target mode should install this newly-released package, which adds this enhancement.

3.13. RHEA-2011:1727 — NEW PACKAGE: PYTHON-SIMPLEPARSE

A new python-simpleparse package is now available for Red Hat Enterprise Linux 6.

The python-simpleparse package is a simple and fast parser generator for the Python programming environment.

This enhancement update adds the python-simpleparse package to Red Hat Enterprise Linux 6 as part of the Technology Preview of Fibre Channel over Ethernet (FCoE) target mode. (BZ#726776)

IMPORTANT

This package is provided as a dependency of the fcoe-target-utils package. It is recommended to install it only as a prerequisite for running fcoe-target-utils, and not to use it independently.

All users who want to use the Technology Preview of Fibre Channel over Ethernet target mode should install this newly-released package, which adds this enhancement.

3.14. RHEA-2012:0022 — NEW PACKAGE: PYTHON-SUDS

The python-suds package is now available for Red Hat Enterprise Linux 6 Server and Red Hat Enterprise Linux High Performance Compute Node.

The python-suds package provides a lightweight implementation of the Simple Object Access Protocol (SOAP) for the Python programming environment.

This enhancement update adds the python-suds package to Red Hat Enterprise Linux 6 Server and Red Hat Enterprise Linux High Performance Compute Node. Previously it was only available with the Red Hat Enterprise Linux High Availability and Red Hat Enterprise Linux Resilient Storage add-on products.

(BZ#765896)

All users who require python-suds are advised to install this new package.

3.15. RHEA-2011:1622 — NEW PACKAGE: PYTHON-SUDS

A new python-suds package is now available for Red Hat Enterprise Linux 6.

The python-suds package provides a lightweight implementation of the Simple Object Access Protocol (SOAP) for the Python programming environment.

This enhancement update adds the python-suds package to Red Hat Enterprise Linux 6. (BZ#681835)

All users who require python-suds are advised to install this new package.

3.16. RHEA-2011:1726 — NEW PACKAGE: PYTHON-URWID

A new python-urwid package is now available for Red Hat Enterprise Linux 6.

The python-urwid package provides a library for development of text user interface applications in the Python programming environment.

This enhancement update adds the python-urwid package to Red Hat Enterprise Linux 6 as part of the Technology Preview of Fibre Channel over Ethernet (FCoE) target mode. (BZ#726775)

IMPORTANT

This package is provided as a dependency of the fcoe-target-utils package. It is recommended to install it only as a prerequisite for running fcoe-target-utils, and not to use it independently.

All users who want to use the Technology Preview of Fibre Channel over Ethernet target mode should install this newly-released package, which adds this enhancement.

3.17. RHEA-2011:1590 — NEW PACKAGE: SANLOCK

A new sanlock package is now available for Red Hat Enterprise Linux 6.

The sanlock package provides a shared disk lock manager that uses disk paxos to manage leases on shared storage. Hosts connected to a common Storage Area Network (SAN) can use sanlock to synchronize the access to the shared disks. Both libvirt and vdsm can use sanlock to synchronize access to shared virtual machine (VM) images.

This enhancement update adds the sanlock package to Red Hat Enterprise Linux 6. (BZ#658971)

All users who require sanlock are advised to install this new package.

3.18. RHEA-2011:1640 — NEW PACKAGES: SGABIOS

New sgabios packages are now available for Red Hat Enterprise Linux 6.

The sgabios packages provide the Google Serial Graphics Adapter BIOS (SGABIOS) for legacy 86-bit software to communicate with an attached serial console.

This enhancement update adds the new sgabios packages to Red Hat Enterprise Linux 6. (BZ#725832)

All users who require SGABIOS are advised to install these new packages.

3.19. RHEA-2011:1610 — NEW PACKAGES: SPICE-GTK

New spice-gtk packages are now available for Red Hat Enterprise Linux 6.

spice-gtk is a GTK2 widget for SPICE clients. Both virt-manager and virt-viewer can make use of this widget to access virtual machines using the SPICE protocol.

This enhancement update adds spice-gtk to Red Hat Enterprise Linux 6. (BZ#708417)

All users of SPICE clients such as virt-manager or virt-viewer are advised to install these new packages.

3.20. RHEA-2011:1633 — NEW PACKAGE: TBOOT

A new tboot package is now available for Red Hat Enterprise Linux 6.

The tboot package provides Trusted Boot (tboot), an open source pre- kernel/VMM module, that uses Intel Trusted Execution Technology (Intel TXT) to initialize the launch of a operating system kernels and virtual machines.

This enhancement update adds tboot to Red Hat Enterprise Linux 6. (BZ#691617)

All users wishing to evaluate trusted boot capabilities are advised to install this new package.

3.21. RHEA-2011:1752 — NEW PACKAGE: VIOS-PROXY

A new vios-proxy package is now available as a Technology Preview for Red Hat Enterprise Linux 6.

The vios-proxy program suite creates a network tunnel between a server in the QEMU host and a client in a QEMU guest. The proxied server and client programs open normal TCP network ports on localhost and the vios-proxy tunnel connects them using QEMU virtioserial channels.

This enhancement update adds a new vios-proxy package to Red Hat Enterprise Linux 6 as a Technology Preview. (BZ#721119)

More information about Red Hat Technology Previews is available here:

https://access.redhat.com/support/offerings/techpreview/

All users who want to use the vios-proxy Technology Preview should install this newly-released package, which adds this enhancement.

3.22. RHEA-2011:1757 — NEW PACKAGE: VIRT-WHO

A new virt-who package is now available for Red Hat Enterprise Linux 6.

The virt-who package provides an agent that collects information about virtual guests present in the system and reports them to the Red Hat Subscription Manager tool.

This enhancement update adds the virt-who package to Red Hat Enterprise Linux 6. (BZ#725832)

All users are advised to install this new package.

3.23. RHEA-2011:1625 — NEW PACKAGE: WDAEMON

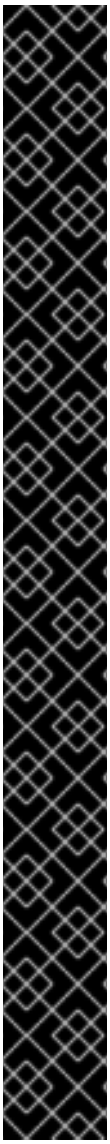
A new wdaemon package is now available for Red Hat Enterprise Linux 6.

The new wdaemon package contains a daemon to wrap input driver hotplugging in the X.Org implementation of the X Window System server. The wdaemon package emulates virtual input devices to avoid otherwise non-persistent configuration of Wacom tablets to persist across device removals.

This enhancement update adds the wdaemon package to Red Hat Enterprise Linux 6.

All users who require wdaemon should install this new package.

CHAPTER 4. PACKAGE UPDATES



IMPORTANT

The Red Hat Enterprise Linux 6 Technical Notes compilations for Red Hat Enterprise Linux 6.0, 6.1 and 6.2 have been republished.

Each compilation still lists all advisories comprising their respective GA release, including all Fastrack advisories.

To more accurately represent the advisories released between minor updates of Red Hat Enterprise Linux, however, some advisories released asynchronously between minor releases have been relocated.

Previously, these asynchronously released advisories were published in the Technical Notes for the most recent Red Hat Enterprise Linux minor upate. Asynchronous advisories released after the release of Red Enterprise Linux 6.1 and before the release of Red Hat Enterprise Linux 6.2 were published in the Red Hat Enterprise Linux 6.2 Technical Notes, for example.

Most of these asynchronous advisories were concerned with, or even specific to, the then extant Red Hat Enterprise Linux release, however.

With these republished Technical Notes, such advisories are now incorporated into the Technical Notes for the Red Hat Enterprise Linux release they are associated with.

Future Red Hat Enterprise Linux Technical Notes will follow this pattern. On first publication a Red Hat Enterprise Linux X.y Technical Notes compilation will include the advisories comprising that release along with the Fastrack advisories for the release.

Upon the GA of the succeeding Red Hat Enterprise Linux release, the Red Hat Enterprise Linux X.y Technical Notes compilation will be republished to include associated asynchronous advisories released since Red Hat Enterprise Linux X.y GA up until the GA of the successive release.

4.1. 389-DS-BASE

4.1.1. RHEA-2011:1711 — 389-ds-base bug fix and enhancement update

Updated 389-ds-base packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The 389 Directory Server is an LDAPv3 compliant server. The base packages include the Lightweight Directory Access Protocol (LDAP) server and command-line utilities for server administration.

Bug Fixes

BZ#720458

If a server sent a response to an unbind request and the client simply closed the connection, Directory Server 8.2 logged "Netscape Portable Runtime error -5961 (TCP connection reset by peer.)".

BZ#752155

An incorrect SELinux context caused AVC errors in /var/log/audit/audit.log.

BZ#697663, BZ#700665, BZ#711533, BZ#711241, BZ#726136, BZ#700215

A number of memory leaks and performance errors were fixed.

BZ#711266

The DS could not restart after a new object class was created which used the entryUSN attribute.

BZ#712167

The ns-slapd process segfaulted if suffix referrals were enabled.

BZ#711513

A high volume of TCP traffic could cause the slapd process to quit responding to clients.

BZ#714298

Attempting to delete a VLV index caused the server to hang.

BZ#720051

Connections to the DS by an RSA authentication server using simple paged results by default would timeout.

BZ#735217

Running a simple paged search against a subtree with a host-based ACI would hang the server.

BZ#733443

If the target attribute list for an ACI had syntax errors and more than five attributes, the server crashed.

BZ#734267

It was not possible to set account lockout policies after upgrading from RHDS 8.1.

BZ#720452

Adding an entry with an RDN containing a % caused the server to crash.

BZ#709868

Only FIPS-supported ciphers can be used if the server is running in FIPS mode.

BZ#711265

It is possible to disable SSLv3 and only allow TLS.

BZ#713317, BZ#713318

If the changelog was encrypted and the certificate became corrupt, the server crashed.

BZ#733434

If the passwordisglobalpolicy attribute was enabled on a chained server, a secure connection to the master failed.

BZ#714310

If a chained database was replicated, the server could segfault.

BZ#694571

Editing a replication agreement to use SASL/GSS-API failed with GSS-API errors.

BZ#742611

In replication, a msgid may not be sent to the right thread, which caused "Bad parameter to an LDAP routine" errors. This causes failures to propagate up and halt replication.

BZ#701057

Password changes were replicated among masters replication, but not to consumers.

BZ#717066

If an entry was modified on RHDS and the corresponding entry was deleted on the Windows side, the sync operation attempts to use the wrong entry.

BZ#734831

Some changes were not properly synced over to RHDS from Windows.

BZ#726273

RHDS entries were not synced over to Windows if the user's CN had a comma.

BZ#718351

Intensive update loads on master servers could break the cache on the consumer, causing it to crash.

BZ#699458

Syncing a multi-valued attribute could delete all the other instances of that attribute when a new value was added.

BZ#729817

If a synced user subtree on Windows was deleted and then a user password was changed on the RHDS, the DS would crash.

Enhancements

BZ#742382

The nsslapd-idlistscanlimit configuration attribute can be set dynamically, instead of requiring a restart.

BZ#742661

Separate resource limits can be set for paged searches, independent of resource limits for regular searches.

BZ#720459

The sudo schema has been updated.

BZ#739959

A new configuration attribute sets a different list of replicated attributes for a total update versus an incremental update.

BZ#733440

A new configuration option allows the server to be started with an expired certificate.

BZ#720461

New TLS/SSL error messages have been added to the replication error log level.

Users are advised to upgrade to these updated 389-ds-base packages, which resolve these issues and add these enhancements.

4.1.2. RHBA-2012:0049 — 389-ds-base bug fix update

Updated 389-ds-base packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The 389-ds-base packages provide 389 Directory Server, which is an LDAPv3 compliant server. The base packages include the Lightweight Directory Access Protocol (LDAP) server and command-line utilities for server administration.

Bug Fixes

BZ#758682

When the LDAP server was under a heavy load, and the network was congested, client connections could experience problems. If there was a connection problem while the server was sending Simple Paged Result (SPR) search results to the client, the LDAP server called a cleanup routine incorrectly. This led to a memory leak and the server terminated unexpectedly. With this update, the underlying code has been modified to ensure that cleanup tasks are run correctly and memory leaks no longer occur. The LDAP server no longer crashes in this scenario.

BZ#758683

Previously, certain operations with the Change Sequence Number (CSN) were not very effective in 389 Directory Server. Therefore, performing a large number of the modrdn operations during Directory Server content replications led to poor performance, and the ns-slapd daemon consumed up to 100% CPU under these circumstances. With this update, the underlying code has been modified to use these CSN operations efficiently so that replications in Directory Server now work as expected in this scenario.

BZ#758688

Previously, allocated memory was not correctly released in the underlying code for the SASL GSSAPI authentication method, when checking the Simple Authentication and Security Layer (SASL) identity mappings. This problem could cause memory leaks when processing SASL bind requests, which eventually caused the LDAP server to terminate unexpectedly with a segmentation fault. This update adds function calls that are needed to free allocated memory correctly. Memory leaks no longer occur and the LDAP server no longer crashes in this scenario.

BZ#771631

Previously, 389 Directory Server used the Netscape Portable Runtime (NSPR) implementation of the read/write locking mechanism. This implementation allowed deadlocks to occur if 389 Directory Server was under a heavy load, which caused the server to become unresponsive. With this update, 389 Directory Server now uses the POSIX implementation of the locking mechanism, and deadlocks no longer occur under a heavy load.

BZ#771632

Under a heavy load in replicated environments, 389 Directory Server did not handle the Entry USN index correctly. Consequently, the index could become out of sync with the main database and search operations on USN entries returned incorrect results. This update modifies the Entry USN plug-in and 389 Directory Server now handles the Entry USN index as expected.

All users of 389-ds-base are advised to upgrade to these updated packages, which fix these bugs.

4.2. ABRT AND LIBREPORT

4.2.1. RHBA-2011:1598 — abrt and libreport bug fix and enhancement update

Updated abrt and libreport packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The abrt packages contain the Automatic Bug Reporting Tool (ABRT) version 2. In comparison with ABRT version 1, this version provides more flexible configuration, which covers a variety of customer use cases that the previous version was unable to cover. It also moves a lot of data processing from the daemon to separate tools that run without root privileges, which makes the daemon less error prone and the whole processing more secure.

Note: This update obsoletes the former report tool and replaces the report library to unify the reporting process in all Red Hat applications (Anaconda, setroubleshoot, ABRT). The most interesting feature for end-users is the problem solution searching: when ABRT is configured to report to the Red Hat Customer Portal, it tries to search Red Hat problem databases (such as Knowledge Base or Bugzilla) for possible solutions and refers the user to these resources if the solution is found.

Bug Fixes

BZ#610603

The abrt-gui application used to list plug-ins multiple times if they were configured in the configuration file. This is now fixed.

BZ#627621

In the previous version of ABRT, a daemon restart was required for any changes in the configuration to take effect. In the new version, most of the options in the configuration file no longer require a restart.

BZ#653872

Support for retrace server has been added. Refer to https://fedorahosted.org/abrt/wiki/AbrtRetraceServer for more information about this new feature.

BZ#671354

By default, ABRT stores all problem information in the /var/spool/abrt/ directory. Previously, this path was hard coded and could not be changed in the configuration. With this update, this path can be changed in the /etc/abrt/abrt.conf configuration file.

BZ#671359

The previous documentation failed to cover some customer use cases. This error has been fixed, and all of these use cases are now covered in the Red Hat Enterprise Linux 6 Deployment Guide.

BZ#673173

In ABRT version 1, it was not possible to use wildcards to specify that some action should happen for any user. ABRT version 2 adds support for this functionality.

BZ#695416

The lacking information about configuring a proxy has been added to the Red Hat Enterprise Linux 6 Deployment Guide.

BZ#707950

Previously, a bug in ABRT version 1 was preventing a local Python build to finish. This is now fixed.

BZ#725660

The previous report tool and report library have been obsoleted by abrt and libreport. Users can notice the change in the problem reporting user interface of Anaconda, setroubleshoot, and ABRT.

All users of ABRT are advised to upgrade to these updated packages, which provide numerous bug fixes and enhancements.

4.3. ACL

4.3.1. RHBA-2011:0924 — acl bug fix update

Updated acl packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Access Control Lists (ACLs) are used to define finer-grained discretionary access rights for files and directories. The acl packages contain the getfacl and setfacl utilities needed for manipulating access control lists.

Bug Fixes

BZ#674883

Prior to this update, the setfacl.1 man page was not intelligible in that it did not state that removing a non-existent ACL entry is not considered to be an error. With this update, the setfacl.1 man page has been updated so that its content is now intelligible and exactly specifies the aforementioned behavior with regard to removing a non-existent ACL entry.

BZ#702638

Prior to this update, the package specification did not reflect a change of the upstream project web page address. This update corrects the respective address in the package specification.

All users of Access Control Lists should upgrade to these updated packages, which fix these bugs.

4.3.2. RHEA-2011:1657 — acl enhancement update

Updated acl packages that add two enhancements are now available for Red Hat Enterprise Linux 6.

Access Control Lists (ACLs) are used to define finer-grained discretionary access rights for files and directories. The acl packages contain the getfacl and setfacl utilities needed for manipulating access control lists.

Enhancements

BZ#720318

Prior to this update, the ACL library did not provide any function to check for extended ACLs of a file without following symbolic links. The only available function, acl_extended_file(), used to cause unnecessary mounts of autofs. This update introduces a new function, acl_extended_file_nofollow(), that checks for extended ACLs of a file without following symbolic links.

BZ#723998

Previously, the ACL library was linked without support for RELRO (read-only relocations) flags. With this update, the library is now linked with partial RELRO support.

Users of acl are advised to upgrade to these updated packages, which add these enhancements.

4.4. AIDE

4.4.1. RHBA-2012:0512 — aide bug fix update

Updated aide packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Advanced Intrusion Detection Environment (AIDE) is a program that creates a database of files on a system, and then uses that database to ensure file integrity and detect system intrusions.

Bug Fix

BZ#811936

Previously, the aide utility incorrectly initialized the gcrypt library. This consequently prevented aide to initialize its database if the system was running in FIPS-compliant mode. The initialization routine has been corrected, and along with an extension to the libgcrypt's API introduced in the RHEA-2012:0486 advisory, aide now initializes its database as expected if run in a FIPS-compliant way.

All users of aide are advised to upgrade to these updated packages, which fix this bug.

4.5. ALSA-LIB

4.5.1. RHBA-2011:1719 — alsa-lib bug fix update

Updated alsa-lib packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The alsa-lib packages contain libraries for the Advanced Linux Sound Architecture (ALSA).

Bug Fix

BZ#704772

Prior to this update, the alsa output plugin for the Audacious Audio Player did not work correctly. As a result, Audacious could under certain circumstances fail to generate any sound and display error messages. With this update, alsa-lib is modified so that Audacious can now generate sound as expected.

All alsa-lib users are advised to upgrade to these updated packages, which fix this bug.

4.6. ANACONDA

4.6.1. RHBA-2011:1565 — anaconda bug fix and enhancement update

An updated anaconda package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The anaconda package contains portions of the Anaconda installation program that can be run by the user for reconfiguration and advanced installation options.

Bug Fixes

BZ#641861

Issues with "interactive" mode partitioning are fixed.

BZ#731274

The network command is parsed correctly.

BZ#689996

The /boot partition on EFI systems is handled correctly.

BZ#705274

Files that are necessary for libreport and SSL installation mode have been added.

BZ#676404

Symbolic links to LVM commands have been added to the rescue image.

BZ#730650

The /sbin/cio_ignore command is added to initrd.img for IBM System z.

BZ#689029

Support for dracut-style "rdloaddriver=" and "rdblacklist=" parameters is added.

BZ#679108

Support for static addresses in "ipv6=" is added.

BZ#706099

A testing framework for stub commands is added.

BZ#699745

Driver disks support multiple kernel versions and are also built for Red Hat Enterprise Linux 6.0 and 6.1.

BZ#668570

Network connection is brought up before saving a bug report.

BZ#715130

Errors in .treeinfo are detected.

BZ#698282

The xhost authentication is changed when performing live installation.

BZ#664981, BZ#726804

Debugging improvements in loader and package installation code have been made.

BZ#679810

The dialog box focus and initialization have been corrected.

BZ#701220

The iSCSI Login button is disabled when no nodes are selected.

BZ#695362

When a mount point is set to /boot, the file system type is no longer changed.

BZ#728280, BZ#725777, BZ#723194, BZ#723344, BZ#694800, BZ#621175

EDD handling improvements have been made, including Xen and CCISS.

BZ#698429

Extended partitions are handled correctly.

BZ#681803

Handling of "network --device=bootif" is corrected.

BZ#750764

Centering of the Anaconda window when an external display is present is corrected.

BZ#605938

Encrypted device lines written to kickstart files are corrected.

BZ#618535

zFCP multipath devices can be added in the user interface as expected.

BZ#732380

iSCSI discovery that returns no devices is handled correctly.

BZ#704593

Systems with more than 2147483647 kB of memory are handled properly.

BZ#712487

The header image is hidden on all but 800x600 displays.

BZ#690058

The "noprobe" parameter for driver disks is honored.

BZ#713991

The "linksleep=" boot parameter is honored.

BZ#699640

Installation sources (including NFS ISO storages) are mounted correctly.

BZ#679397

Processes in the anaconda process group are killed when the system is shut down.

BZ#693271

Partitioning alignment is corrected.

BZ#616641

Progress indicator improvements for device discovery and command line mode have been made.

BZ#691817, BZ#690748

Kickstart network failures and device name collisions are handled properly.

BZ#691910

The "crashkernel=" parameter in a kickstart file is handled properly.

BZ#712195

Support for the "ext4migrate" parameter has been removed.

BZ#706675

The language and keyboard selection screens are now skipped in stage2 when possible.

BZ#614504

Device capacity values are sorted as numbers, not characters.

BZ#695740

Swap partitions are handled correctly.

BZ#676118

The "--target" option is used in kickstart files for iSCSI devices.

BZ#701371, BZ#696876, BZ#674241, BZ#734374, BZ#729716

Various multipath and raid storage bugs are fixed.

BZ#679073

Anaconda verifies that devices specified with "part" can be partitioned.

Enhancements

BZ#659790

Vendor-provided tools on driver disks are now allowed.

BZ#694198

The initrd.img file is compressed with LZMA.

BZ#696696

The "noverifyssl" boot parameter is added.

BZ#697419

The tboot package is configured when it is installed.

BZ#709653

Multipath device can now be specified using WWID.

Users of anaconda should upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.7. APR

4.7.1. RHBA-2012:0740 — apr bug fix update

An updated apr package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. It provides a free library of C data structures and routines.

Bug Fix

BZ#830265

Previously, a bug in the handling of IPv6 sockets was present in the apr_mcast_hops() function. This bug could have prevented applications from successfully using multicast with IPv6 sockets. With this update, this bug has been fixed so that the applications now operate correctly.

All APR users are advised to install this newly released package, which fixes this bug.

4.8. AT

4.8.1. RHBA-2012:0068 — at bug fix update

An updated at package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The "at" package provides the at and "batch" commands, which are used to read commands from standard input or from a specified file. The "at" command allows you to specify that a command will be run at a particular time. The "batch" command will execute commands when the system load levels drop to a particular level. Both commands use the /bin/sh.

Bug Fix

BZ#783190

Due to an error in the time-parsing routine, the "at" command incorrectly calculated the year when a job was scheduled by using days on input. For example: "at now + 10 days". This update fixes erroneous grammar so that "at" now schedules jobs correctly.

All users of at are advised to upgrade to this updated package, which fixes this bug.

4.9. ATLAS

4.9.1. RHEA-2011:1582 — atlas enhancement update

Updated atlas packages that add various enhancements are now available for Red Hat Enterprise Linux 6.

The ATLAS (Automatically Tuned Linear Algebra Software) project is a research effort focusing on applying empirical techniques providing portable performance. The atlas packages provide C and Fortran77 interfaces to a portably efficient BLAS (Basic Linear Algebra Subprograms) implementation and routines from LAPACK (Linear Algebra PACKage).

The atlas packages have been upgraded to upstream version 3.8.4, which adds a number of enhancements over the previous version. The atlas package now contains subpackages optimized for Linux on IBM System z architectures. (BZ#694459)

All users of atlas are advised to upgrade to these updated packages, which add these enhancements.

4.10. ATTR

4.10.1. RHBA-2011:1272 — attr bug fix update

Updated attr packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The attr packages provide extended attributes, which can be used to store system objects like capabilities of executables and access control lists, as well as user objects.

Bug Fixes

BZ#651119

Prior to this update, the setfattr utility could not restore the original values of the attributes when the "getfattr -e text" or "getfattr --encoding=text" command was used to dump attributes with embedded null characters. This update fixes the encoding of these values in getfattr to prevent information loss.

BZ#665049

Prior to this update, the getfattr utility followed symbolic links to directories even if the "-h" or "--no-dereference" option was specified. Additionally, the description in the getfattr(1) man page that related to this functionality was misleading. This update fixes getfattr with the "-h" option so that it no longer follows the symbolic links and the related content of the getfattr(1) man page is now correct.

BZ#665050

Prior to this update, the getfattr utility did not return a non-zero exit code when an attribute specified in the "getfattr" command did not exist. This update fixes getfattr so that it now returns a non-zero exit code when an attribute does not exist.

BZ#674870

Prior to this update, supported methods for encoding values of the extended attributes were not properly described in the setfattr(1) man page. This update adds the appropriate descriptions of the encoding methods to the setfattr(1) man page.

BZ#702639

Prior to this update, the project web page address as stated in the package specification did not reflect the change of the upstream project web page address. This update corrects the project web page address in the package specification.

BZ#727307

Prior to this update, the attr library was built without support for read-only relocations (RELRO) flags. With this update, the library is now built with partial RELRO support.

All users of attr are advised to upgrade to these updated packages, which fix these bugs.

4.11. AUDIT

4.11.1. RHBA-2011:1739 — audit bug fix and enhancement update

Updated audit packages that fix various bugs and add several enhancements are now available for Red Hat Enterprise Linux 6.

The audit packages contain the user space utilities for storing and searching the audit records which have been generated by the audit subsystem in the Linux 2.6 kernel.

The audit package has been upgraded to upstream version 2.1.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#731723)

Bug Fixes

BZ#715279

Previously, the audit daemon was logging messages even when configured to ignore "disk full" and "disk error" actions. With this update, audit now does nothing if it is set to ignore these actions, and no messages are logged in the described scenario.

BZ#715315

Previously, the Audit remote logging client received a "disk error" event instead of "disk full" event from a server when the server's disk space ran out. This bug has been fixed and the logging client now returns the correct event in the described scenario.

BZ#748124

Prior to this update, the audit system was identifying the accept4() system call as the now deprecated paccept() system call. Now, the code has been fixed and audit uses the correct identifier for the accept4() system call.

BZ#709345

Previously, the "auditctl -l" command returned 0 even if it failed because of dropped capabilities. This bug has been fixed and a non-zero value is now returned if the operation is not permitted.

BZ#728475

When Kerberos support was disabled, some configuration options in the audisp-remote.conf file related to Kerberos 5 generated warning messages about GSSAPI support during boot. With this update, the options are now commented out in the described scenario and the messages are no longer returned.

BZ#700005

On i386 and IBM System z architectures, the "autrace -r /bin/ls" command returned error messages even though all relevant rules were added correctly. This bug has been fixed and no error messages about sending add rule data requests are now returned in the described scenario.

All audit users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.12. AUGEAS

4.12.1. RHEA-2011:1659 — augeas bug fix and enhancement update

Updated augeas packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Augeas is a configuration editing tool. Augeas parses configuration files in their native formats and transforms them into a tree. Configuration changes are made by manipulating this tree and saving it back into native config files.

The augeas packages have been upgraded to upstream version 0.9.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#691483)

Bug Fix

BZ#693539

Previously, due to a bug in the source code, parsing invalid files failed silently without any error message. With this update, error messages are provided to inform users about the problem.

All users of Augeas are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.13. AUTOFS

4.13.1. RHBA-2011:1723 — autofs bug fix and enhancement update

An updated autofs package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

Bug Fixes

BZ#704935

The autofs utility did not reset the map entry status on a reload request. As a result, newly added map entries that had previously recorded a mount failure failed to work. With this update, autofs resets the map entry status on a reload request and map entries are mounted as expected.

BZ#704939

The autofs utility could have terminated with a segmentation fault when attempting certain mounts. This occurred due to a race condition between mount handling threads for mounts that had previously recorded a mount failure. The automount cache map entry is now verified to be valid.

BZ#704940

The automount(8) man page referred to a non-existent man page. This was caused by a typographical error in the code. With this update, the man page reference has been corrected and the man page is displayed as expected.

BZ#704929

Due to a deadlock, autofs could stop responding when attempting to mount map entries that were nested within maps. With this update, the underlying code has been changed and, where possible, nested map entries mount correctly.

BZ#704933

Prior to this update, automount could terminate unexpectedly with a pthreads error. This occurred because attempts to acquire the master map lock occasionally failed as the lock was held by another thread. With this update, the underlying code has been adapted to wait for a short time before failing.

BZ#704928, BZ#704927

When retrieving paged results from an LDAP (Lightweight Directory Access Protocol) server, autofs handled certain cases incorrectly, which caused the query to not obtain all results. This update adds the code that handles these additional cases.

BZ#704937

Prior to this update, if a key entry of an automount map began with an asterisk (*) sign, the daemon failed with a segmentation fault because the sign was not matched correctly. With this update, such asterisk signs are handled correctly.

BZ#704228

When using GSSAPI authentication, the fact that an incorrect authentication host name was being used caused the connection to fail. This update now gets the correct host name for the connection.

BZ#692816

automount was not performing sufficient sanity checks of server names in its configuration. This update corrects the configuration entry parsing.

BZ#700136

Error reporting for invalid mount locations was unclear. This update improves the error reporting.

BZ#703332

When an automount map key is present in a file map and is also present in an included map source, if the file map entry was removed and a lookup performed before a re-load was issued, the map lookup would have failed. This update corrects the logic used to determine if the lookup needs to continue into included maps.

BZ#718927

When reloading maps that include a combination of direct and indirect maps, it was possible for automount to deadlock due to incorrect lock ordering.

BZ#

There was inadvertent use of a small amount of GPLv3-licensed code from Samba in autofs. While this was permissible, it would have entailed explicitly relicensing autofs from "GPLv2 or later" to "GPLv3", which is not intended for autofs at this time. Therefore, the Samba-derived code has been replaced in order to maintain the "GPLv2 or later" licensing status of autofs.

Enhancements

BZ#704416

This update adds the "--dumpmaps" option to the automount command, which allows you to dump the maps from their source as seen by the automount daemon.

BZ#704932

This update adds simple Base64 encoding for LDAP and thus allows hashing of the password entries in the /etc/autofs_ldap_auth.conf configuration file.

All autofs users are advised to upgrade to this updated package, which provides numerous bug fixes and enhancements.

4.13.2. RHBA-2012:0320 — autofs bug fix update

An updated autofs package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

Bug Fix

BZ#787122

A function to check validity of a mount location was meant to check only for a small subset of map location errors. A recent improvement modification in error reporting inverted a logic test in this validating function. Consequently, the scope of the test was widened, which caused automount to report false positive failures. With this update, the faulty logic test has been corrected and false positive failures no longer occur.

All users of autofs are advised to upgrade to this updated package, which fixes this bug.

4.14. AUTOTRACE

4.14.1. RHBA-2011:1168 — autotrace bug fix update

Updated autotrace packages that fix one bug are now available for Red Hat Enterprise Linux 6.

AutoTrace is a program for converting bitmaps to vector graphics. Supported input formats include BMP, TGA, PNM, PPM, and any format supported by ImageMagick, whereas output can be produced in PostScript, SVG, xfig, SWF, and others.

Bug Fix

BZ#658057

When installing autotrace-devel multilib RPM packages from the optional repository, file conflicts between these packages appeared, causing the installation transaction to abort. This problem has been fixed and the installation transaction now proceeds without conflicts.

All users of autotrace are advised to upgrade to these updated packages, which resolve this issue.

4.15. BACULA

4.15.1. RHBA-2011:1232 — bacula bug fix update

Updated bacula packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

Bacula is a set of programs that allow you to manage the backup, recovery, and verification of computer data across a network of different computers.

Bug Fixes

BZ#651776

Prior to this update, the bacula packages were not distributed with the applybaculadate file. As a result, the logwatch cron script failed. The problem has been fixed by including the applybaculadate file in the bacula packages so that the logwatch cron script now works as expected.

BZ#651780

Prior to this update, the make_catalog_backup.pl script created a MySQL configuration file, which had the file permissions set to world-writeable and world-readable so that MySQL did not accept the configuration file with these permissions and the MySQL database login configuration was not used. As a result, it was not possible to complete a MySQL database dump. With this update, the configuration file is now created with correct permissions, and the MySQL database login configuration is used by MySQL so that it is now possible to complete the MySQL database dump as expected.

BZ#651786

Prior to this update, there was no option to change Bacula's runtime user. As a consequence, Bacula was always run under the root user. The problem has been fixed by adding support for the bacula-dir, bacula-fd, and bacula-sd files in the /etc/sysconfig/ directory; these files can be used for specifying a non-root user and group with the DIR_USER, FD_USER, SD_USER, and DIR_GROUP, FD_GROUP and SD_GROUP options, respectively. With this update, Bacula can be run under the specified user.

BZ#651787

Prior to this update, when creating a symbolic link to the "bscan" utility, the new link was erroneously named "dbcheck". As a result, the already existing "dbcheck" symbolic link was overwritten by the erroneous one. Thus the "dbcheck" command ran the "bscan" utility so that it was not possible to execute the "bscan" utility with the "bscan" command. The problem has been fixed in this update so that the "dbcheck" and "bscan" utilities now work as expected.

BZ#657297

Prior to this update, Bacula's default configuration missed a required option. As a result, the Bacula tray monitor component terminated unexpectedly. The problem has been fixed by adding the "Address" option to the "Director" section in the Bacula tray monitor configuration file so that the Bacula tray monitor now works as expected with the default configuration file. Note that this bug fix does not alter any existing Bacula tray monitor configuration file. As a consequence, the Bacula tray monitor can terminate unexpectedly if the existing Bacula tray monitor configuration is incorrect.

BZ#689400

Prior to this update, the backup size was computed incorrectly under certain circumstances. As a consequence, the reported size of the incremental backup could have been wrong. The problem has been fixed by correcting the backup size computation process so that the size of the incremental backup is now reported correctly.

BZ#712794

Prior to this update, the shadow-utils package was not listed among the package dependencies for Bacula. As a result, the bacula user and bacula group were not created when the shadow-utils package was not present on the system, and a warning message was displayed during the bacula packages installation. This bug has been fixed by adding shadow-utils to the package dependencies.

BZ#712804

Prior to this update, the chkconfig package, which contains the "alternatives" utility, was not listed among the package dependencies for Bacula. As a result, the bacula-dir and bacula-sd services were not configured, the "alternatives" utility was not found, and Bacula's symbolic links were not created. These problems have been fixed by adding chkconfig to the package dependencies.

All users of Bacula are advised to upgrade to these updated packages, which fix these bugs.

4.16. BASH

4.16.1. RHBA-2012:0561 — bash bug fix update

Updated bash packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The GNU Bourne Again shell (Bash) is a shell and command language interpreter compatible with the Bourne shell (sh). Bash is the default shell for Red Hat Enterprise Linux.

Bug Fix

BZ#814271

When a SIGCHLD signal was received in job control mode and a handler for the signal was installed, Bash called the trap handler within the signal handler itself. This was unsafe and could cause Bash to enter a deadlock or to terminate unexpectedly with a segmentation fault due to memory corruption. With this update, the trap handler is now called outside of the signal handler, and Bash no longer enters a deadlock, neither crashes in this scenario.

All users of bash are advised to upgrade to these updated packages, which fix this bug.

4.17. BFA-FIRMWARE

4.17.1. RHBA-2011:1759 — bfa-firmware bug fix and enhancement update

An updated bfa-firmware package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The bfa-firmware package contains the Brocade Fibre Channel Host Bus Adapter (HBA) Firmware to run Brocade Fibre Channel and CNA adapters. This package also supports the Brocade BNA network adapter.

The bfa-firmware package has been upgraded to upstream version 3.0.0.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#735142)

All users of Brocade Fibre Channel and CNA adapters are advised to upgrade to this updated package, which fixes several bugs and adds various enhancements.

4.18. BIND

4.18.1. RHSA-2012:0716 — Important: bind security update

Updated bind packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Security Fixes

CVE-2012-1667

A flaw was found in the way BIND handled zero length resource data records. A malicious owner of a DNS domain could use this flaw to create specially-crafted DNS resource records that would cause a recursive resolver or secondary server to crash or, possibly, disclose portions of its memory.

CVE-2012-1033

A flaw was found in the way BIND handled the updating of cached name server (NS) resource records. A malicious owner of a DNS domain could use this flaw to keep the domain resolvable by the BIND server even after the delegation was removed from the parent DNS zone. With this update, BIND limits the time-to-live of the replacement record to that of the time-to-live of the record being replaced.

Users of bind are advised to upgrade to these updated packages, which correct these issues. After installing the update, the BIND daemon (named) will be restarted automatically.

4.18.2. RHBA-2011:1697 — bind bug fix update

Updated bind packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.

Bug Fixes

BZ#699951

Prior to this update, the code in libdns which sends DNS requests was not robust enough and suffered from a race condition. If a race condition occurred, the "named" name service daemon logged an error message in the format "zone xxx.xxx.xxx.in-addr.arpa/IN: refresh: failure trying

master xxx.xxx.xxx.xxx#53 (source xxx.xxx.xxx.xxx#0): operation canceled" even when zone refresh was successful. This update improves the code to prevent a race condition in libdns and the error no longer occurs in the scenario described.

BZ#700097

A command or script traditionally gives a non-zero exit status to indicate an error. Prior to this update, the nsupdate utility incorrectly returned the exit status "0" (zero) when the target DNS zone did not exist. Consequently, the nsupdate command returned "success" even though the update failed. This update corrects this error and nsupdate now returns the exit status "2" in the scenario described.

BZ#725577

Prior to this update, named did not unload the bind-dyndb-ldap plugin in the correct places in the code. Consequently, named sometimes terminated unexpectedly during reload or stop when the bind-dyndb-ldap plugin was used. This update corrects the code, the plug-in is now unloaded in the correct places, and named no longer crashes in the scenario described.

BZ#693982

A non-writable working directory is a long time feature on all Red Hat systems. Previously, named wrote "the working directory is not writable" as an error to the system log. This update changes the code so that named now writes this information only into the debug log.

BZ#717468

The named initscript lacked the "configtest" option that was available in earlier releases. Consequently, users of the bind initscript could not use the "service named configtest" command. This update adds the option and users can now test their DNS configurations for correct syntax using the "service named configtest" command.

All users of bind are advised to upgrade to these updated packages, which fix these bugs.

4.18.3. RHBA-2011:1836 — bind bug fix update

Updated bind packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with the DNS server); and tools for verifying that the DNS server is operating properly.

Bug Fixes

BZ#758669

Prior to this update, errors arising on automatic updates of DNSSEC trust anchors were handled incorrectly. Consequently, the named daemon could become unresponsive on shutdown. With this update, the error handling has been improved and named exits on shutdown gracefully.

BZ#758670

Prior to this update, a race condition could occur on validation of DNSSEC-signed NXDOMAIN responses and the named daemon could terminate unexpectedly. With this update, the underlying code has been fixed and the race condition no longer occurs.

All users of bind are advised to upgrade to these updated packages, which fix these bugs.

4.18.4. RHBA-2012:0009 — bind bug fix update

Updated bind packages that fix one bug are now available for Red Hat Enterprise Linux 6.

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with the DNS server); and tools for verifying that the DNS server is operating properly.

Bug Fix

BZ#769366

The multi-threaded named daemon uses the atomic operations feature to speed-up an access to shared data. This feature did not work correctly on the 32-bit and 64-bit PowerPC architectures. Therefore, the named daemon sometimes became unresponsive on these architectures. This update disables the atomic operations feature on the 32-bit and 64-bit PowerPC architectures, which ensures that the named daemon is now more stable, reliable and no longer hangs.

All users of bind are advised to upgrade to these updated packages, which fix this bug.

4.19. BIND-DYNDB-LDAP

4.19.1. RHSA-2012:0683 — Important: bind-dyndb-ldap security update

An updated bind-dyndb-ldap package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The dynamic LDAP back end is a plug-in for BIND that provides back-end capabilities to LDAP databases. It features support for dynamic updates and internal caching that help to reduce the load on LDAP servers.

Security Fix

CVE-2012-2134

A flaw was found in the way bind-dyndb-ldap handled LDAP query errors. If a remote attacker were able to send DNS queries to a named server that is configured to use bind-dyndb-ldap, they could trigger such an error with a DNS query leveraging bind-dyndb-ldap's insufficient escaping of the LDAP base DN (distinguished name). This would result in an invalid LDAP query that named would retry in a loop, preventing it from responding to other DNS queries. With this update, bind-dyndb-ldap only attempts to retry one time when an LDAP search returns an unexpected error.

Red Hat would like to thank Ronald van Zantvoort for reporting this issue.

All bind-dyndb-ldap users should upgrade to this updated package, which contains a backported patch to correct this issue. For the update to take effect, the named service must be restarted.

4.19.2. RHBA-2011:1715 — bind-dyndb-ldap bug fix update

An updated bind-dyndb-ldap package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The dynamic LDAP (Lightweight Directory Access Protocol) back end is a plug-in for BIND that provides an LDAP database back-end capabilities. It features support for dynamic updates and internal caching to lift the load off of the LDAP server.

Bug Fixes

BZ#742368

Previously, the bind-dyndb-ldap plug-in could faile to honor the selected authentication method because it did not call the ldap_bind() function on reconnection. Consequently, the plug-in connected to the LDAP server anonymously. With this update, the ldap_bind() function is executed on reconnection and the plug-in uses the correct authentication method in the described scenario.

BZ#707255

The bind-dyndb-ldap plug-in failed to load new zones from the LDAP server runtime. This update adds the zone_refresh parameter to the plug-in which controls how often the zone check is performed.

BZ#745045

The bind-dyndb-ldap plug-in could fail to connect to the LDAP server. This happened when the LDAP server was using localhost and FreeIPA installation was using a name different from the machine hostname. This update adds to the plug-in the ldap_hostname option, which can be used to set the correct LDAP server hostname.

BZ#727856

The "named" process could have remained unresponsive due to a race condition in the bind-dyndb-ldap plug-in. With this update, the race condition has been resolved and the problem no longer occurs.

All users of bind-dyndb-ldap are advised to upgrade to this updated package, which fixes these bugs.

4.20. BINUTILS

4.20.1. RHBA-2011:1523 — binutils bug fix and enhancement update

An updated binutils package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assemblers), gprof (for displaying call graph profile data), ld (the GNU linker), nm (for listing symbols from object files), objcopy (for copying and translating object files), objdump (for displaying information from object files), ranlib (for generating an index for the contents of an archive), readelf (for displaying detailed information about binary files), size (for listing the section sizes of an object or archive file), strings (for listing printable strings from files), strip (for discarding symbols), and addr2line (for converting addresses to file and line).

Bug Fixes

BZ#664640

Prior to this update, the **readelf** utility added **`0x40`** into a character in order to display a non-printing

character but did not do so when processing a multibyte character. As a result, the **readelf** utility did not display a multibyte character in the ELF header correctly. The code has been corrected and readelf no longer displays garbled characters when processing multibyte, or non-ASCII, characters.

BZ#674925

An unneeded patch to **bineutils** caused a large link time degradation when using the **`binutils --build-id`** command. This update removes that patch.

BZ#689829

An *Operating System* (OS) *Application Binary Interface* (ABI) describes the low-level interface between a program and the operating system (OS/ABI). The indirect meta-function, **`ifunc()`**, whose value can be determined at load time, allows for architecture dependent optimization. Prior to this update, the OS/ABI preprocessor macro was erroneously set to **`UNIX - Linux`** instead of **`UNIX - System V`** in an ELF header by a dynamic executable which used **`ifunc()`**. This update applies a backported patch which corrects the code and the error no longer occurs.

BZ#698005

Prior to this update, the binutils' **`strip`** command, which is run as part of the RPM build process, did not copy the **`EI_OSABI`** value in the ELF file header properly, it set the value to zero. Consequently, if the **`EI_OSABI`** field of the debug file had a value of **`3`** (ABI tag for GNU/Linux), in the stripped file it was erroneously set to **`0`** (**`UNIX - System V`**). This update corrects the problem and **`strip`** now leaves the field intact.

BZ#701586

On 64-bit PowerPC platforms, the position of ***`-ldl`*** in the list compiler options caused unexpected behavior when compiling C++ code. If ***`-ldl`*** was not placed at the end of parameter list, the GNU C Compiler (GCC) failed with an error in the format:

```
libtest.a(some_object_file.o): undefined reference to `.dlerror'
```

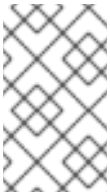
With this update, the code has been corrected and the GCC compiler functions as expected.

BZ#707387

When compiling C source code using the GNU C Compiler (GCC), a Table Of Contents (TOC), is created for every executable file. Prior to this update, compiling C++ code using GCC for 64-bit PowerPC, using **`-mcmodel=small -mno-minimal-toc`** as options, GNU linker, (**ld**), erroneously decided that if a section did not make use of the TOC it could belong to any TOC group. Consequently, when a local function call was made from one section of code to another section in the same object file, due to the two sections being assigned to different TOC groups, a failure occurred and an error message in the following format was logged.

```
libbackend.a(cse.o)(.text.unlikely+0x60): sibling call optimization to
`.opd' does not allow automatic multiple TOCs; recompile with -mminimal-
toc or -fno-optimize-sibling-calls, or make `.opd' extern
```

This update applies an upstream patch to improve the partitioning of sections of code, which make local function calls, into multiple TOC groups. As a result the error no longer occurs in the scenario described.



NOTE

It is necessary to relink executables and shared libraries containing objects which were compiled with **`-mcmodel=small -mno-minimal-toc`**. Therefore code should be recompiled by running these commands again after applying the update.

BZ#714824

Prior to this update, after compiling a kernel from source code with debugging information, some debug information was missing. Consequently, when using the GNU Project's debugger (GDB) utility, if a user issued the command **`l setup_arch`** to determine the target architecture, the following error was displayed.

```
No line number known for setup_arch
```

This update corrects the code and the GDB utility now correctly displays the architecture for which the code was compiled.

BZ#721079

Compilers used for producing code optimized for 64-bit PowerPC platforms use the default Red Hat Enterprise Linux system linker, **ld**, provided with the operating system to produce executables and libraries. Some object code generated by the IBM XL compiler caused **ld** to terminate unexpectedly with a segmentation fault. Consequently, users were not able to produce optimized executables or libraries. With this update, a backported patch has been applied to correct the problem and **ld** no longer crashes in the scenario described.

BZ#733122

When linking FORTRAN programs with the IBM XL compiler and the default Red Hat Enterprise Linux 6.1 system linker, **ld** sometimes terminated unexpectedly with a segmentation fault. This updates applies an upstream patch to correct the problem and **ld** no longer crashes in the scenario described.

BZ#747695

The assembler, **as**, when generating a memory reference to a local symbol plus or minus an offset, did not include the constant offset when generating 32-bit x86 code. Consequently, when the local symbol being referenced was defined before the instruction using the symbol with an offset, an error would occur. This update corrects the code and the problem no longer occurs.

Enhancements

BZ#696368

With this update, backported patches have been included to support new AMD processors.

BZ#696494

Certain Intel processors support a new **RdRand** instruction to generate a true random number in a short time. This update includes support for this new instruction.

Users of binutils are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.21. BIOSDEVNAME

4.21.1. RHBA-2011:1608 — biosdevname bug fix and enhancement update

An updated biosdevname package that fixes several bugs and adds various enhancements are now available for Red Hat Enterprise Linux 6.

The biosdevname package contains an optional convention for naming network interfaces; it assigns names to network interfaces based on their physical location. The package is disabled by default, except for a limited set of Dell PowerEdge, C Series and Precision Workstation systems.

The biosdevname package has been upgraded to upstream version 0.3.11, which provides a number of bug fixes and enhancements over the previous version. (BZ#696203)

Bug Fixes

BZ#700248

When NPAR (NIC Partitioning) is enabled, the partition number should be appended as a suffix to the interface name. Previously, biosdevname did not add partition numbers to interface names, for example, instead of naming an interface "em3_1", the interface was named "em3". Consequently, partitioned network interfaces were missing the suffix necessary to describe the partition. Now, biosdevname correctly recognizes the VPD (Vital Product Data) suffix and full interface names are created correctly.

BZ#700251

When biosdevname ran in a guest environment, it suggested names to new network interfaces as if it was in a host environment. Consequently, affected network interfaces were incorrectly renamed. Now, biosdevname no longer suggests names in the described scenario.

BZ#729591

When biosdevname was reading VPD information to retrieve NPAR-related data, the read operations failed or became unresponsive on certain RAID controllers. Additionally, biosdevname sometimes attempted to read beyond the VPD boundary in the sysfs VPD file, which also resulted in a hang. This bug has been fixed and biosdevname now performs the read operation correctly in the described scenarios.

BZ#739592

Previously, the "--smbios" and "--nopirq" command-line parameters were missing in the biosdevname binary. Consequently, consistent network device naming could not be enabled because biosdevname exited without suggesting a name. This update adds support for these parameters and enables the device naming.

BZ#740532

Previously, NICs (Network Interface Cards) on biosdevname-compatible machines were given traditional "eth*" names instead of "em*" or "p*p*" names. This bug has been fixed and biosdevname now provides correct names for the NICs.

Enhancements

BZ#696252

With this update, "--smbios" and "--nopirq" command-line parameters have been added to biosdevname.

BZ#736442

The biosdevname man page has been updated to explain the functionality of the "--smbios" and "--nopirq" command-line parameters.

Users of biosdevname are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.22. BLKTRACE

4.22.1. RHBA-2011:1758 — blktrace bug fix and enhancement update

Updated blktrace packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The blktrace packages contain a number of utilities to record the I/O trace information for the kernel to user space, and utilities to analyze and view the trace information.

Bug Fix

BZ#705128

Prior to this update, the blkparse code contained a misprint. As a result, blkparse used the wrong variable when printing the PC Writes Completed. This update modifies the code so that blkparse now prints the correct value for PC Writes Completed.

Enhancement

BZ#736399

This update adds FLUSH/FUA support to blktrace.

All blktrace users are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

4.23. BLTK

4.23.1. RHBA-2011:1227 — bltk bug fix update

An updated bltk package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The bltk (Battery Life Tool Kit) package includes binaries and scripts to test battery life.

Bug Fixes

BZ#618308

Prior to this update, the bltk tree was corrupted. As a result, the bltk_report script failed. This update modifies the settings of the bltk root path. Now, the report script works as expected.

BZ#679028

Prior to this update, bltk could be installed without requiring the gnuplot binary. As a result, the bltk_plot script exited with an error message when the gnuplot package was not installed and the charts were shown from measured data. This update requires the gnuplot package for its installation. Now, the bltk_plot script no longer exits with an error.

All bltk users are advised to upgrade to this updated package, which fixes these bugs.

4.24. CACHEFILESD

4.24.1. RHBA-2011:1679 — cachefilesd bug fix update

An updated cachefilesd package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The cachefilesd package manages a kernel module that attempts to improve the performance of selected file systems by using local disk space to cache data read over the network.

Bug Fixes

BZ#660347

Prior to this update, cachefilesd used the wrong log level for cull info messages. As a result, the /var/log/messages file could become overloaded. This update reduces the messages to the debug level. Now, /var/log/messages no longer becomes overloaded.

BZ#723890

Prior to this update, cachefilesd depended on a specific version of the SELinux policy package. As a result, only the nominated version was allowed. This update permits the nominated version and any later versions. Now, the SELinux policy dependency works as expected.

All users of cachefilesd are advised to upgrade to this updated package, which fixes these bugs.

4.25. CERTMONGER

4.25.1. RHBA-2011:1708 — certmonger bug fix update

An updated certmonger package that fixes multiple bugs is now available for Red Hat Enterprise Linux 6.

The certmonger service monitors certificates as the date at which they become invalid approaches, optionally attempting to re-enroll with a supported certificate authority (CA) to keep the services which use the certificates running without incident.

Bug Fixes

BZ#692766

Previously, the certmonger service could access a Network Security Services (NSS) database without a password, despite being configured to use a password to access that database. This behavior was not recognized as an error. This update correctly diagnoses this inconsistency as an error.

BZ#694184

Previously, if the certmonger service could not generate a key pair in an NSS database because it did not have the password that was required for accessing the database, the certmonger service did not recover when it was subsequently given the correct password. This update handles this case correctly.

BZ#697058

Previously, the certmonger service did not correctly diagnose a missing token if the name of the token to use was specified when the service was instructed to generate a key pair for storage in an NSS database. This update corrects this error.

BZ#712500

Previously, the certmonger service encountered an assertion failure if the D-Bus message bus service was not already running when certmonger was started. This update modifies the certmonger service so that no more assertion problems occur in such a situation.

BZ#721392

Previously, when the getcert command needed to report an error message which it received from the certmonger service, it exited unexpectedly due to a logic error. This update corrects the logic so that the error message is correctly reported.

BZ#727863

Previously, the certmonger service was not fully compatible with newer versions of the xmlrpc-c and libcurl packages. As a result, credentials could not be delegated when using GSSAPI authentication with a CA that was accessed via XML-RPC. This update includes the necessary changes to continue to be able to delegate credentials when using GSSAPI authentication with a CA that is accessed using XML-RPC, such as IPA.

BZ#699059, BZ#739903

Previously, when the getcert request command was given a location for key or certificate storage using a relative path, and the location did not exist, the error was only reported after multiple warnings during which the command attempted to convert the relative path to an absolute path. This update suppresses these warnings.

BZ#741262

Previously, an incorrect error message was displayed if the getcert resubmit command was invoked with the -i flag to specify which request should be resubmitted to a CA but no request that matched the provided value was present. This update displays the correct error message.

BZ#742348

Due to a logic error, attempts to save a newly-obtained certificate to an NSS database could fail intermittently. This update corrects the error.

Enhancements

BZ#698772

Previously, the getcert list command only printed information about every certificate and enrollment request being managed by certmonger, and there was no way to narrow down the results. This update includes an updated version of the command which can narrow the result set if the invoking user provides information about the location of the certificate or key in which the user is interested

BZ#750617

This update now includes an HTTP "Referer:" header value when submitting requests to CAs which are accessed using XML-RPC, as is expected to be required by future releases of the IPA CA

All users of the certmonger service are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.26. CHKCONFIG

4.26.1. RHBA-2012:0415 — chkconfig bug fix update

Updated chkconfig packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The basic system utility chkconfig updates and queries runlevel information for system services.

Bug Fixes

BZ#797847

When installing multiple Linux Standard Base (LSB) services which only had LSB headers, the stop priority of the related LSB init scripts could have been miscalculated and set to "-1". With this update, the LSB init script ordering mechanism has been fixed, and the stop priority of the LSB init scripts is now set correctly.

BZ#797846

When an LSB init script requiring the "$local_fs" facility was installed with the "install_initd" command, the installation of the script could fail under certain circumstances. With this update, the underlying code has been modified to ignore this requirement because the "$local_fs" facility is always implicitly provided. LSB init scripts with requirements on "$local_fs" are now installed correctly.

All users of chkconfig are advised to upgrade to these updated packages, which fix these bugs.

4.27. CIFS-UTILS

4.27.1. RHBA-2011:1585 — cifs-utils bug fix update

An updated cifs-utils package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The cifs-utils package contains utilities for mounting and managing CIFS shares.

Bug Fixes

BZ#676439

Prior to this update, mount.cifs dropped the CAP_DAC_READ_SEARCH flag together with most of the other capability flags before it performed a mount. As a result, mounting onto a directory without execute permissions failed if mount.cifs was installed as a setuid program and the user mount was configured in the /etc/fstab file. This update reinstates the CAP_DAC_READ_SEARCH flag before calling mount. Now, mounting no longer fails.

BZ#719363

Prior to this update, several mount options were missing from the mount.cifs(8) man page. With this update, the man page documents all mount options.

All users of cifs-utils are advised to upgrade to this updated cifs-utils package, which fixes these bugs.

4.28. CJKUNI-FONTS

4.28.1. RHBA-2011:0922 — cjkuni-fonts bug fix update

Updated cjkuni-fonts packages that fix one bug are now available for Red Hat Enterprise Linux 6.

CJK Unifonts are Unicode TrueType fonts derived from original fonts made available by Arphic Technology under the Arphic Public License and extended by the CJK Unifonts project.

Bug Fix

BZ#682650

Prior to this update, when viewing the U+4190 CJK character with the AR PL UMing font and the font size 10, this character was not displayed properly. This bug has been corrected in this update so that the character is now correctly displayed as expected.

All users of cjkuni-fonts are advised to upgrade to these updated packages, which fix this bug.

4.29. CLUSTER AND GFS2-UTILS

4.29.1. RHBA-2012:1190 — cluster and gfs2-utils bug fix update

Updated cluster and gfs2-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The Red Hat Cluster Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure. Using redundant hardware, shared disk storage, power management, and robust cluster communication and application failover mechanisms, a cluster can meet the needs of the enterprise market.

Bug Fix

BZ#849048

Previously, it was not possible to specify start-up options to the dlm_controld daemon. As a consequence, certain features were not working as expected. With this update, it is possible to use the /etc/sysconfig/cman configuration file to specify dlm_controld start-up options, thus fixing this bug.

All users of cluster and gfs2-utils are advised to upgrade to these updated packages, which fix this bug.

4.29.2. RHBA-2011:1516 — cluster and gfs2-utils bug fix and enhancement update

Updated cluster and gfs2-utils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The cluster packages contain the core clustering libraries for Red Hat High Availability as well as utilities to maintain GFS2 file systems for users of Red Hat Resilient Storage.

Bug Fixes

BZ#707115

The cluster and gfs2-utils packages have been upgraded to upstream version 3.0.12.1, which provides a number of bug fixes over the previous version.

BZ#713977

Previously, when a custom multicast address was configured, the configuration parser incorrectly set

the default value of the time-to-live (TTL) variable for multicast packet to 0. As a consequence, cluster nodes were not able to communicate with each other. With this update, the default TTL value is set to 1, which fixes the problem.

BZ#726777

A section describing the "suborg" option for the fence_cisco_usc agent was not present in the RELAX NG schema which is used to validate the cluster.conf file. As a consequence, validation of cluster.conf failed even if the file was valid. The suborg section has been added to the RELAX NG schema and cluster.conf is now validated correctly.

BZ#707091

Building the resource group index for a new GFS2 file system using the mkfs.gfs2 utility used all the space allocated. If the file system filled up completely, no room was left to write a new rindex entry. As a consequence, the gfs2_grow utility was unable to expand the file system. The mkfs.gfs2 utility has been modified so that enough space is now allocated for the entire rindex file, and one extra rindex entry. The gfs2_grow source code has been modified to utilize the unused rindex space. As a result, gfs2_grow is now able to expand a completely full GFS2 file system.

BZ#678585

GFS2 POSIX (Portable Operating System Interface) lock operations (implemented in Distributed Lock Manager, also known as DLM) are not interruptible when they wait for another POSIX lock. Previously, processes that created a deadlock with POSIX locks could not be killed to resolve the problem, and one node had to be reset. DLM now uses a new kernel feature that allows the waiting process to be killed, and information about the killed process is now passed to the dlm_controld daemon to be cleaned up. Processes deadlocked on GFS2 POSIX locks can now be recovered by killing one or more of them.

BZ#719135

Prior to this update, boundaries for the locktable and label fields in the GFS2 superblock were not properly checked by the tunegfs2 tool. As a consequence, running the "gfs2_tool sb" command could terminate unexpectedly with buffer overflow. In addition, invalid characters could be printed when using tunegfs2 to change locktable or label to a minimum or maximum length (63 characters). The tunegfs tool has been modified to check the correct boundaries of the locktable and label fields. As a result, tunegfs2 no longer creates invalid locktables or labels, and therefore gfs2_tool prints the superblock values properly.

BZ#740385

When executing the cman utility by using the init script with enabled debugging, a file descriptor leaked. The file pointed to the file descriptor would continue to grow endlessly, filling up the /tmp file system. This update ensures that the file descriptor is closed after a successful cman startup. Space in /tmp is now released correctly.

BZ#695795

The cman utility implements a complex set of checks to configure the Totem protocol. One of the checks that copies the configuration data was incorrect and the transport protocol option was not handled correctly as a consequence. A patch has been applied to address this issue and cman now handles the transport option properly.

BZ#679566

When the user executed the "gfs2_edit savemeta" command to save the metadata for a target GFS2 file system, not all of the directory information was saved for large directories. If the metadata was restored to another device, the fsck.gfs2 tool found directory corruption because of a missing leaf

block. This was due to gfs2_edit treating the directory leaf index (also known as the directory hash table) like a normal data file. With this update, gfs2_edit's savemeta function is modified to actually read all the data (the directory hash table) for large directories and traverse the hash table, saving all the leaf blocks. Now, all leaf blocks are saved properly.

BZ#679080

When the fsck.gfs2 tool was resolving block references and no valid reference was found, the reference list became empty. As a consequence, fsck.gfs2 check in pass1b terminated unexpectedly with a segmentation fault. With this update, pass1b is modified to check that the list is empty. The segmentation fault no longer occurs and fsck.gfs2 proceeds as expected.

BZ#731775

The dlm_controld daemon passed error results back to the kernel for POSIX unlock operations flagged with CLOSE. As a consequence, the kernel displayed the "dlm: dev_write no op" error messages, most of them when using non-POSIX locks, flocks. The dlm_controld daemon has been fixed to not pass error results to the kernel for POSIX unlock operations flagged with CLOSE. As a result, error messages no longer appear.

BZ#729071

Previously, the mount.gfs2 utility passed the "loop" option to the GFS2 kernel module which treated it as an invalid option. Mounting a GFS2 file system on loopback devices failed with an "Invalid argument" error message. With this update, mount.gfs2 is modified to avoid passing the "loop" option to the kernel. Mounting GFS2 systems on loopback devices now works as expected.

BZ#728230

Missing sanity checks related to the length of a cluster name caused the cman utility to fail to start. The correct sanity checks have been implemented with this update. The cman utility starts successfully and informs the user of the incorrect value of the cluster name, if necessary.

BZ#726065

The XML format requires special handling of certain special characters. Handling of these characters was not implemented correctly, which caused the cluster.conf file to not function as expected. Correct handling of the characters has been implemented and cluster.conf now works as expected.

BZ#706141

The exact device/mount paths were not compared due to incorrect logic in mount.gfs2 when trying to find mtab entries for deletion. The original entry was not found during remounts and therefore was not deleted. This resulted in double mtab entries. With this update, the realpath() function is used on the device/mount paths so that they match the content of mtab. As a result, the correct original mtab entry is deleted during a remount, and a replacement entry with the new mount options is inserted in its place.

BZ#720668

Previously, mkfs.gfs2 treated normal files incorrectly as if they were block devices. Attempting to create a GFS2 file system on a normal file caused mkfs.gfs2 to fail with a "not a block device" error message. Additional checks have been added so that mkfs.gfs2 does not call functions specific for block devices on normal files. GFS2 file systems can now be created on normal files. However, use of GFS2 in such cases is not recommended.

BZ#719126

The tunegfs2 command line usage message was not updated to reflect the available arguments which are documented in the man page. As a consequence, tunegfs2 printed an inaccurate usage message. The usage message has been updated and tunegfs2 now prints an accurate message.

BZ#719124

Previously, certain argument validation functions did not return error values, and tunegfs2 therefore printed confusing error messages instead of exiting quietly. Error handling has been improved in these validation functions, and tunegfs2 now exits quietly instead of printing the confusing messages.

BZ#694823

Previously, the gfs2_tool command printed the UUID (Universally Unique Identifier) output in uppercase. Certain applications expecting the output being in lowercase (such as mount) could have malfunctioned as a consequence. With this update, gfs2_tool is modified to print UUIDs in lowercase so that they are in a commonly accepted format.

BZ#735917

The qdisk daemon did not allow cman to upgrade the quorum disk device name. The quorum disk device name was not updated when the device was changed and, in very rare cases, the number of qdiskd votes would therefore not be correct. A new quorum API call has been implemented to update the name and votes of a quorum device. As a result, quorum disk device names and votes are updated consistently and faster than before.

BZ#683104

Prior to this update, the fsck.gfs2 utility used the number of entries in the journal index to look for missing journals. As a consequence, if more than one journal was missing, not all journals were rebuilt and subsequent runs of fsck.gfs2 were needed to recover all the journals. Each node needs its own journal; fsck.gfs2 has therefore been modified to use the "per_node" system directory to determine the correct number of journals to repair. As a result, fsck.gfs2 now repairs all the journals in one run.

BZ#663397

Previously, token timeout intervals of corosync were larger than the time it took a failed node to rejoin the cluster. Consequently, corosync did not detect that a node had failed until it rejoined. The failed node had been added again before the dlm_controld daemon asked corosync for the new member list, but dlm_controld did not notice this change. This eventually caused the DLM (Distributed Lock Manager) lockspace operations to get stuck. With this update, dlm_controld can notice that a node was removed and added between checks by looking for a changed incarnation number. Now, dlm_controld can properly handle nodes that are quickly removed and added again during large token timeouts.

BZ#732991

Previously, if a cluster was configured with a redundant corosync ring, the dlm_controld daemon would log harmless EEXIST errors, "mkdir failed: 17". This update removes these error messages so that they no longer appear.

Enhancements

BZ#733345

The corosync IPC port allows, when configured correctly, non-privileged users to access corosync services. Prior to this update, the cman utility did not handle such connections correctly. As a consequence, users were not able to configure unprivileged access to corosync when it was

executed using cman. This update adds support to cman to configure unprivileged access. As a result, configured users and groups can now access corosync services without root privileges.

BZ#680930

This update introduces dynamic schema generation, which provides a lot of flexibility for end users. Users can plug into Red Hat Enterprise Linux High Availability Add-On custom resource and fence agents, and still retain the possibility to validate their cluster.conf file against those agents.

BZ#732635, BZ#735912

This update adds support for Redundant Ring Protocol, which aligns the default configuration of cman with corosync. Note that this enhancement is included as a Technology Preview.

BZ#702313

Previously, gfs2_edit saved GFS2 metadata uncompressed. Saved GFS2 metadata sets could have filled up a lot of storage space, and transferring them (for example, for support and debugging) would be slow. This update adds gzip compression to the metadata saving and restoring functions of gfs2_edit. GFS2 metadata sets are now compressed when saving and decompressed when restoring them. The user can specify the compression level with a command line option.

BZ#704178

With this update, the tunegfs2 utility replaces the superblock manipulating feature of gfs2_tool.

BZ#673575

Previously, the fence_scsi agent did not reboot a node when it was fenced. As a consequence, the node had to be rebooted manually before rejoining the cluster. This update provides a script for detecting loss of SCSI reservations. This can be used in conjunction with the watchdog package in order to reboot a failed host.

Users of cluster and gfs2-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.29.3. RHBA-2012:0575 — cluster and gfs2-utils bug fix update

Updated cluster and gfs2-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Red Hat Cluster Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure. Using redundant hardware, shared disk storage, power management, and robust cluster communication and application failover mechanisms, a cluster can meet the needs of the enterprise market.

Bug Fix

BZ#820357

Prior to this update, the cmannotifyd did not correctly generate a cluster status notification message at first cluster startup. This update addresses the problem and now cmannotifyd will correctly trigger the notification hooks when the daemon is started.

All users of cluster and gfs2-utils are advised to upgrade to these updated packages, which fix this bug.

4.30. CLUSTERMON

4.30.1. RHEA-2011:1550 — clustermon bug fix update

Updated clustermon packages that fix a bug and add an enhancement are now available for Red Hat Enterprise Linux 6.

The clustermon packages are used for remote cluster management.

Bug Fix

BZ#634373

Previously, the clustermon tool failed to shut down nodes if the user had mounted a GFS2 file system that was not listed in the /etc/fstab file. This was caused by clustermon relying on the rgmanager tool and the GFS2 init scripts to unmount all file systems, but the cluster stack would not stop properly if the user mounted the file system manually. This has been fixed: clustermon now ensures that there are no cluster file systems mounted and then attempts to stop the cluster stack.

Enhancement

BZ#724978

The "get_cluster_schema" function call has been added to allow users to easily get the XML cluster schema content.

All users of clustermon are advised to upgrade to this updated packages, which resolves this bug.

4.31. COOLKEY

4.31.1. RHEA-2011:1738 — coolkey enhancement update

An enhanced coolkey package is now available for Red Hat Enterprise Linux 6.

The coolkey package contains driver support for CoolKey and Common Access Card (CAC) smart card products.

Enhancements

BZ#578690

This update adds support for Personal Identity Verification (PIV) smart cards.

BZ#700907

Common Access Cards (CAC) are defined to have exactly three certificates. However, some cards that used the CAC interface supplied one or two certificates only, which may have caused the coolkey utility to fail. CAC smart cards that contain less than three certificates are now supported.

Users of PIV and CAC smart cards are advised to upgrade to this updated package, which adds these enhancements.

4.32. COREUTILS

4.32.1. RHBA-2011:1693 — coreutils bug fix update

Updated coreutils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The coreutils packages contain the core GNU utilities. These packages combine the old GNU fileutils, sh-utils, and textutils packages.

Bug Fixes

BZ#691292

Prior to this update, SELinux appeared to be disabled when building coreutils in Mock. As a result, coreutils did not build. With this update, SELinux determines more precisely whether it is disabled or not. Now, the packages are built successfully.

BZ#703712

Previously, incorrect signal handling could cause various problems for tcsh users logging into the root shell using the su utility. Signal masking in the subshell called by the su utility has been modified to respect the SIGTSTP signal as well as the SIGSTOP signal.

BZ#715557

When using the "-Z/--context" option in the cp utility, the SELinux context of a file was not changed if the file destination already existed. The utility has been modified and the context is changed as expected. However, this option is not portable to other systems.

BZ#720325

Prior to this update, the acl_extended_file() function could cause unnecessary mounts of autofs when using the ls command on a directory with autofs mounted. This update adds the new acl function, acl_extended_file_nofollow(), to prevent unnecessary autofs mounts.

BZ#725618

The description of the "--sleep-interval" option in the tail(1) manual page has been improved to be clearer about the behavior and to match the upstream version of coreutils.

All users of coreutils are advised to upgrade to these updated packages, which fix these bugs.

4.33. COROSYNC

4.33.1. RHBA-2012:1214 — corosync bug fix update

Updated corosync packages that fix a bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The corosync packages provide the Corosync Cluster Engine and C Application Programming Interfaces (APIs) for Red Hat Enterprise Linux cluster software.

Bug Fix

BZ#849553

Previously, the corosync-notifyd daemon, with dbus output enabled, waited 0.5 seconds each time a message was sent through dbus. Consequently, corosync-notifyd was extremely slow in producing output and memory of the Corosync server grew. In addition, when corosync-notifyd was killed, its

memory was not freed. With this update, corosync-notifyd no longer slows down its operation with these half-second delays and Corosync now properly frees memory when an IPC client exits.

Users of corosync are advised to upgrade to these updated packages, which fix this bug.

4.33.2. RHBA-2011:1515 — corosync bug fix and enhancement update

Updated corosync packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The corosync packages provide the Corosync Cluster Engine and C Application Programming Interfaces (APIs) for Red Hat Enterprise Linux cluster software.

Bug Fixes

BZ#677583

Prior to this update, the corosync-blackbox command could, under certain circumstances, produce a backtrace in the output and consequently terminate with a segmentation fault. With this update, Corosync creates correct fdata files and also corosync-fplay is more resistant when dealing with incorrect fdata files.

BZ#677583

Prior to this update, cpg did not use the "left_nodes" field in the downlist message. As a consequence, a node could miss a configuration change and report larger old_members than expected if one node was paused. This update modifies the downlist so that the "left_nodes" field is used. Now, the membership events are correct.

BZ#692620

Prior to this update, cpg did not use the "left_nodes" field in the downlist message. As a consequence, a node could miss a configuration change and report larger old_members than expected if one node was paused. This update modifies the downlist so that the "left_nodes" field is used. Now, the membership events are correct.

BZ#696883

Prior to this update, running Corosync could cause a segmentation fault on multiple nodes when executed via CMAN. This update modifies the code so that executing Corosync via CMAN no longer causes segmentation faults with the pacemaker test suite.

BZ#696887

Prior to this update, the reference counting on the configuration server in Corosync was incorrect. As a consequence, terminating the corosync-cfgtool -r command before completing caused a segmentation fault. This update adds the correct reference counting for each architecture. Now, Corosync no longer encounters segmentation faults in this situation.

BZ#707860

Prior to this update, Corosync could terminate with a segmentation fault if it ran out of available open files. This update handles the maximum number of open files more gracefully. Now, Corosync no longer crashes when going over open file limits.

BZ#707867

Prior to this update, corosync-objctl could not create a new object/key and display double or float values. This update adds float and double support to corosync-objctl. Now, corosync-objctl can display object values with double or float types.

BZ#707873

Prior to this update, Corosync could terminate with a segmentation fault if it encountered a negative value for the message type on systems where char is signed. This update improves the check of the message type for incoming messages.

BZ#707875

Prior to this update, an error message was wrongly displayed if files in the service.d directory differed from the service key. With this update, Corosync longer checks for sub parameters in files in the service.d directory. Now, files in service.d directory can contain every possible configuration option.

BZ#709758

Prior to this update, Corosync used a spinlock around I/O operations. As a consequence, Corosync consumed an extremely high portion of the central processing unit (CPU) when running a large amount of inter-process communication (IPC) operations because the spinlocks would spin during I/O. This update replaces the spinlock with a mutual exclusion (mutex), which releases the processor from spinning but enforces correct behavior.

BZ#712115

Prior to this update, an incorrect mutex in the internal confdb data storage system could, under certain circumstances, cause Corosync to terminate with a segmentation fault. This update corrects the mutex and objdb API iteration no longer causes Corosync to terminate with a segmentation fault.

BZ#712188

Prior to this update, Corosync became locked with contrived test cases when the tracking functionality of the internal object database was enabled if it was under heavy load. This update modifies Corosync so that the tracking functionality under heavy load no longer causes Corosync to lock up.

BZ#725058

Prior to this update, retransmit list errors could occur on slower hardware due to high multicast traffic and slow CPU usage. This update processes the multicast buffer queue more frequently and retransmit errors are now less probable.

BZ#732698

Prior to this update, Corosync sometimes terminated unexpectedly when Corosync ran the cman_tool join and cman_tool leave commands in a loop. This update modifies the code so that no more segmentation faults occur in such situations.

Enhancements

BZ#529136

Prior to this update, the protocol in Corosync unnecessarily copied memory on AMD64 and EM64T architectures to align data structures for architectures which do not handle alignment correctly. As a consequence, the utilization of the central processing unit (CPU) was increased. This update can conditionally avoid copies on unaligned safe architectures such as Intel 80386, AMD64, and EM64T architectures. Now the CPU utilization is reduced by around 20%.

BZ#599327

Prior to this update, no diagnostic message was available when the multicast was blocked. As a consequence, each partition lost quorum which never remerged. This update displays a diagnostic warning that the node can not exit the GATHER state when a local NIC (network interface card) fault occurs or the firewall prevents totem from forming a cluster. In addition, the runtime.totem.pg.mrp.srp.firewall_enabled_or_nic_failure key is now set to 1.

BZ#667652

Prior to this update, fenced nodes where not safely powered up due to issues with the boot sequence. As a consequence, users had to skip cluster services at boot to avoid problems such as long response times and fences in two-node clusters. With this update, setting the nocluster boot parameter prevents Corosync to start automatically.

BZ#688260

Prior to this update, configuring two rings with different IP subnets only duplicated the IP address data of one ring. This update adds support for the redundant ring functionality to Corosync as a Technology Preview.

BZ#707876

Prior to this update, the corosync init script did not depend on syslog. As a consequence, syslog logging did not work if the user turned off syslog. This update adds syslog as a dependency to the init script. Now, logging works in all cases.

BZ#722469

Prior to this update, configuring two rings with different IP subnets only duplicated the IP address data of one ring. This update adds support for the redundant ring functionality to Corosync as a Technology Preview.

All **corosync** users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.33.3. RHBA-2012:0373 — corosync bug fix update

Updated corosync packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The corosync packages provide the Corosync Cluster Engine and C Application Programming Interfaces (APIs) for Red Hat Enterprise Linux cluster software.

Bug Fix

BZ#791236

Previously, the range condition for the update_aru() function could cause incorrect check of message IDs. Due to this, in rare cases, the corosync utility entered the "FAILED TO RECEIVE" state, and so failed to receive multicast packets. With this update, the range value in the update_aru() function is no longer checked for; the fail_to_recv_const constant performs such checks. Now, corosync does not fail to receive packets.

All users of corosync are advised to upgrade to these updated packages, which fix this bug.

4.33.4. RHBA-2012:0536 — corosync bug fix update

Updated corosync packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The corosync packages provide the Corosync Cluster Engine and the C language APIs for Red Hat Enterprise Linux cluster software.

Bug Fix

BZ#810917

Previously, the underlying library of corosync did not delete temporary buffers used for Inter-Process Communication (IPC) that are stored in the /dev/shm shared memory file system. Therefore, if the user without proper privileges attempted to establish an IPC connection, the attempt failed with an error message as expected but memory allocated for temporary buffers was not released. This could eventually result in /dev/shm being fully used and Denial of Service. This update modifies the coroipcc library to let applications delete temporary buffers if the buffers were not deleted by the corosync server. The /dev/shm file system is no longer cluttered with needless data in this scenario and IPC connections can be established as expected.

All users of corosync are advised to upgrade to these updated packages, which fix this bug.

4.33.5. RHBA-2012:0737 — corosync bug fix update

Updated corosync packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The corosync packages provide the Corosync Cluster Engine and C Application Programming Interfaces (APIs) for Red Hat Enterprise Linux cluster software.

Bug Fix

BZ#828432

Previously, it was not possible to activate or deactivate debug logs at runtime due to memory corruption in the objdb structure. With this update, the debug logging can now be activated or deactivated on runtime, for example with the command "corosync-objctl -w logging.debug=off".

All users of corosync are advised to upgrade to these updated packages, which fix this bug.

4.33.6. RHBA-2013:0724 — corosync bug fix update

Updated corosync packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The Corosync packages provide the Corosync Cluster Engine and C Application Programming Interfaces (APIs) for Red Hat Enterprise Linux cluster software.

Bug Fix

BZ#929098

When running applications which used the Corosync IPC library, some messages in the dispatch() function were lost or duplicated. This update properly checks the return values of the dispatch_put() function, returns the correct remaining bytes in the IPC ring buffer, and ensures that the IPC client is correctly informed about the real number of messages in the ring buffer. Now, messages in the dispatch() function are no longer lost or duplicated.

Users of corosync are advised to upgrade to these updated packages, which fix this bug.

4.34. CPUFREQUTILS

4.34.1. RHBA-2011:1224 — cpufrequtils bugfix update

An updated cpufrequtils package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The cpufrequtils package contains utilities that can be used to control the cpufreq interface provided by the kernel on hardware that supports CPU frequency scaling.

Bug Fix

BZ#675734

Prior to this update, the cpufreq-aperf utility did not run on 32-bit systems due to an incorrect argument passed to the read() call. This problem has been fixed: the buffer size is now used instead of the size of the pointer and the cpufreq-aperf utility runs as expected.

All users of cpufrequtils are advised to upgrade to this updated package, which resolves this bug.

4.35. CRASH

4.35.1. RHBA-2011:1648 — crash bug fix and enhancement update

An updated crash package that fixes various bugs and adds several enhancements is now available for Red Hat Enterprise Linux 6.

The crash package provides a self-contained tool that can be used to investigate live systems, and kernel core dumps created from the netdump, diskdump, kdump, and Xen/KVM "virsh dump" facilities from Red Hat Enterprise Linux.

BZ#710193

The crash package has been upgraded to upstream version 5.1.8, which provides a number of enhancements and bug fixes over the previous version.

Bug Fixes

BZ#705142

Previously, compressed kdump dump files were handled incorrectly on AMD64 and Intel 64 architectures if a system contained more than 454 CPUs. In such a case, the crash session terminated during initialization with the "crash: compressed kdump: invalid nr_cpus value: [cpus]" error message. A patch has been provided to address this issue, and the compressed dump files are now handled properly, thus fixing this bug.

BZ#716931

When the first chunk of physical memory on a system was assigned to NUMA (Non-Uniform Memory Architecture) node 1 (typically it is assigned to NUMA node 0), the "kmem -s" or "kmem -S" command incorrectly showed all cache blocks allocated by the slab allocator as empty. This bug has been fixed, and the kmem command now shows populated kmem_cache slab data correctly.

BZ#712214

In a rare scenario, a non-crashing CPU received a shutdown NMI (non-maskable interrupt) immediately after receiving an interrupt from another source. Because the IRQ entry-point symbols "IRQ0x00_interrupt" through "IRQ0x##_interrupt" no longer existed, the bt command terminated with the "bt: cannot transition from exception stack to current process stack" error message on AMD64 and Intel 64 architectures. This bug has been fixed, and backtrace now properly transitions from the NMI stack back to the interrupted process stack.

Enhancements

BZ#695413

The crash.8 man page and the associated built-in "crash -h" output have been re-written. The crash.8 man page now clarifies the required invocation options, adds all of the rarely-used command line options that have proliferated over the years, and updates the ENVIRONMENT variables section. The "crash -h" output now closely mimics the relevant parts of the crash.8 man page.

BZ#703467

With this update, the new "--osrelease [dump_file]" command line option that displays the OSRELEASE vmcoreinfo string from a kdump dump file has been added.

Users of crash are advised to upgrade to this updated package which fixes these bugs and adds these enhancements.

4.36. CRONTABS

4.36.1. RHBA-2011:0872 — crontabs bug fix update

An updated crontabs package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The crontabs package contains root crontab files and directories. You will need to install the cron daemon to run the jobs from crontabs. The cron daemon such as cronie or fcron checks the crontab files to see when particular commands are scheduled to be executed. If commands are scheduled, it executes them. Crontabs handles a basic system function, so it should be installed on your system.

Bug Fix

BZ#609544

Prior to this update, an example included in the /etc/crontab file contained an omission. It did not state that defining a job in crontab requires a username to be defined. The missing information has been added to the /etc/crontab file in this update.

All users of crontabs are advised to upgrade to this updated package, which fixes this bug.

4.37. CRYPTSETUP-LUKS

4.37.1. RHBA-2011:1688 — cryptsetup-luks bug fix and enhancement update

Updated cryptsetup-luks packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

The cryptsetup-luks packages provide a utility which allows users to set up encrypted devices with the Device Mapper and the dm-crypt target.

Bug Fixes

BZ#713410

When the cryptsetup or libcryptsetup utility was run in FIPS (Federal Information Processing Standards) mode, the "Running in FIPS mode." message was displayed during initialization of all commands. This sometimes caused minor issues with associated scripts. This bug has been fixed and the message is now displayed only in verbose mode.

BZ#732179

Prior to this update, several directives were missing in cryptsetup status command implementation. Therefore, the cryptsetup status command always returned the exit code 0 when verifying the status of a mapped device. To fix this issue, the code has been modified. The cryptsetup status command now returns the 0 value only if the device checked is active.

Enhancement

BZ#701936

Previously, the libcryptsetup crypt_get_volume_key() function allowed to perform an action not compliant with FIPS. To conform FIPS requirements, the function is now disabled in FIPS mode and returns an EACCES error code to indicate it. Note that the "luksDump --dump-master-key" command and the key escrow functionality of the volume_key package are also disabled in FIPS mode as a consequence of this update.

All users of cryptsetup-luks are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.38. CTDB

4.38.1. RHBA-2011:1574 — ctdb bug fix and enhancement update

Updated ctdb packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The ctdb packages provide a clustered database based on Samba's Trivial Database (TDB) used to store temporary data.

The ctdb packages have been upgraded to upstream version 1.0.114, which provides a number of bug fixes over the previous version. (BZ#701944)

Bug Fix

BZ#728545

Prior to this update, the ctdb daemon leaked a file descriptor to anon_inodefs. This update modifies ctdb so that this file discriptor can no longer leak.

Enhancement

BZ#672641

This update adds support for Clustered Samba on top of GFS2 as a Technology Preview.

All users of ctdb are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.39. CUPS

4.39.1. RHSA-2011:1635 — Low: cups security and bug fix update

Updated cups packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems.

Security Fix

CVE-2011-2896

A heap-based buffer overflow flaw was found in the Lempel-Ziv-Welch (LZW) decompression algorithm implementation used by the CUPS GIF image format reader. An attacker could create a malicious GIF image file that, when printed, could possibly cause CUPS to crash or, potentially, execute arbitrary code with the privileges of the "lp" user.

Bug Fixes

BZ#681836

Previously CUPS was not correctly handling the language setting LANG=en_US.ASCII. As a consequence lpadmin, lpstat and lpinfo binaries were not displaying any output when the LANG=en_US.ASCII environment variable was used. As a result of this update the problem is fixed and the expected output is now displayed.

BZ#706673

Previously the scheduler did not check for empty values of several configuration directives. As a consequence it was possible for the CUPS daemon (cupsd) to crash when a configuration file contained certain empty values. With this update the problem is fixed and cupsd no longer crashes when reading such a configuration file.

BZ#709896

Previously when printing to a raw print queue, when using certain printer models, CUPS was incorrectly sending SNMP queries. As a consequence there was a noticeable 4-second delay between queueing the job and the start of printing. With this update the problem is fixed and CUPS no longer tries to collect SNMP supply and status information for raw print queues.

BZ#712430

Previously when using the BrowsePoll directive it could happen that the CUPS printer polling daemon (cups-polld) began polling before the network interfaces were set up after a system boot. CUPS was then caching the failed hostname lookup. As a consequence no printers were found and the error,

"Host name lookup failure", was logged. With this update the code that re-initializes the resolver after failure in cups-polld is fixed and as a result CUPS will obtain the correct network settings to use in printer discovery.

BZ#735505

The MaxJobs directive controls the maximum number of print jobs that are kept in memory. Previously, once the number of jobs reached the limit, the CUPS system failed to automatically purge the data file associated with the oldest completed job from the system in order to make room for a new print job. This bug has been fixed, and the jobs beyond the set limit are now properly purged.

BZ#744791

The cups init script (/etc/rc.d/init.d/cups) uses the daemon function (from /etc/rc.d/init.d/functions) to start the cups process, but previously it did not source a configuration file from the /etc/sysconfig/ directory. As a consequence, it was difficult to cleanly set the nice level or cgroup for the cups daemon by setting the NICELEVEL or CGROUP_DAEMON variables. With this update, the init script is fixed.

All users of CUPS are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the cupsd daemon will be restarted automatically.

4.39.2. RHBA-2012:0418 — cups bug fix update

Updated cups packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar operating systems.

Bug Fix

BZ#803419

Previously, empty jobs could be created using the "lp" command either by submitting an empty file to print (for example by executing "lp /dev/null") or by providing an empty file as standard input. In this way, a job was created but was never processed. With this update, creation of empty print jobs is not allowed, and the user is now informed that no file is in the request.

All users of cups are advised to upgrade to these updated packages, which fix this bug.

4.40. CURL

4.40.1. RHBA-2012:0430 — curl bug fix update

Updated curl packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The curl packages provide the libcurl library and the cURL command line tool for transferring data using various protocols, including HTTP, FTP, FILE, LDAP, TELNET, TFTP, SCP. Both, libcurl and cURL, support many useful capabilities, such as user authentication, proxy support, FTP uploading, HTTP POST and PUT methods, SSL certificates, and file transfer resume.

Bug Fixes

BZ#800903

Previously, SSL connections could not be established with libcurl if the selected Network Security

Services (NSS) database was broken or invalid. This update modifies the code of libcurl to initialize NSS without a valid database, which allows applications to establish SSL connections as expected in this scenario.

BZ#800904

The OpenLDAP suite was recently modified to use NSS instead of OpenSSL as the SSL back end. This change led to collisions between libcurl and OpenLDAP on NSS initialization and shutdown. Consequently, applications that were using both, libcurl and OpenLDAP, failed to establish SSL connections. This update modifies libcurl to use the same NSS API as OpenLDAP, which prevents collisions from occurring. Applications using OpenLDAP and libcurl can now connect to the LDAP server over SSL as expected.

All users of curl are advised to upgrade to these updated packages, which fix these bugs. All running applications that use libcurl have to be restarted for this update to take effect.

4.41. CVS

4.41.1. RHSA-2012:0321 — Moderate: cvs security update

Updated cvs packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Concurrent Version System (CVS) is a version control system that can record the history of your files.

Security Fix

CVE-2012-0804

A heap-based buffer overflow flaw was found in the way the CVS client handled responses from HTTP proxies. A malicious HTTP proxy could use this flaw to cause the CVS client to crash or, possibly, execute arbitrary code with the privileges of the user running the CVS client.

All users of cvs are advised to upgrade to these updated packages, which contain a patch to correct this issue.

4.42. CYRUS-IMAPD

4.42.1. RHBA-2012:0708 — cyrus-imapd bug fix update

Updated cyrus-imapd packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The cyrus-imapd packages contain a high-performance mail server with IMAP, POP3, NNTP, and SIEVE support.

Bug Fix

BZ#818209

Previously, the idled daemon incorrectly used signals for communication with the imapd daemon. This could cause a user's mailbox to become unresponsive. To prevent this problem, idled no longer uses signals to communicate with imapd; the AF_UNIX datagram sockets are now used instead.

All users of cyrus-imapd are advised to upgrade to these updated packages, which fix this bug.

4.43. CYRUS-SASL

4.43.1. RHBA-2011:1687 — cyrus-sasl bug fix and enhancement update

Updated cyrus-sasl packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The cyrus-sasl packages contain the Cyrus implementation of the Simple Authentication and Security Layer (SASL), a method for adding authentication support to connection-based protocols.

Bug Fixes

BZ#720451

Prior to this update, the ntlm plug-in did not work due to a code error. This update modifies the source code so that the plug-in now works as expected.

BZ#730242

Prior to this update, creating the user ID and the group ID of the saslauth daemon caused conflicts. This update corrects this behavior and now the saslauth daemon works as expected.

BZ#730246

Prior to this update, cyrus-sasl displayed redundant warnings during the compilation. With this update, cyrus-sasl has been modified and now works as expected.

Enhancement

BZ#727274

This update adds support of partial Relocation Read-Only (RELRO) for the cyrus-sasl libraries.

All users of cyrus-sasl are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.44. DEVICE-MAPPER-MULTIPATH

4.44.1. RHBA-2011-1527 — device-mapper-multipath bug fix and enhancement update

Updated device-mapper-multipath packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

Bug Fixes

BZ#677449

DM Multipath removed a device if it failed to check the device status due to insufficient memory. This happened because the command checking if the device map existed failed as the system returned an error. With this update, Multipath no longer returns an error under these circumstances and no devices are removed if the system runs out of memory while checking device status.

BZ#678673

If a device-mapper-multipath device was open but all attached device paths had been lost, the device was unable to create a new table with no device paths. As a concequence the **`multipath -ll`** command returned output indicating that no paths to the device were available with confusing "failed faulty running" rows presenting the missing paths. Multipath devices now reload tables with no device paths correctly.

BZ#689504

Device paths could fail even if unavailable only temporarily. This happened because the RDAC (Redundant Disk Array Controller) checker function did not recheck the status of hosts if it had received a temporary error code. The function now rechecks the path after it has received such error codes and the path failures are transient as expected.

BZ#697386

A previous bug fix introduced a race condition between the main thread and the thread running the checkerloop routine as the checkerloop thread was created with deferred cancellation type. The checkerloop thread continued running and attempted to access a property, which had been previously unallocated by the main thread. This caused the multipathd daemon to shutdown with a segmentation fault. Now the checkerloop thread checks if a shutdown is in progress and the deamon shuts down gracefully.

BZ#700169

The Multipath daemon failed to include some ghost paths when counting the number of active paths; however, when the ghost paths failed, they were subtracted from the number of active paths. This caused multipathd to fail IO requests even though some paths were still available. The Multipath daemon now counts ghost paths correctly and no longer fails IO requests while there are still active paths available.

BZ#705854

If the user set dev_loss_tmo to a value greater than 600 in **`multipath.conf`** without setting the fast_io_fail_tmo value, the multipathd daemon did not notify the user that fast_io_fail_tmo was not set. Multipath now issues a warning that fast_io_fail_tmo is not set under such circumstances.

BZ#706555

On shared-storage multipath setups that set failback to **`manual`**, multipath could keep alternating from the failover pathgroup to the primary pathgroup infinitely. This happened because multipath was incorrectly failing back to the primary pathgroup whenever a path priority changed. With this update, multipath no longer fails back to the primary pathgroup when a path's priority changes under such circumstances.

BZ#707560

If the multipath device was deleted while a path was being checked, **`multipathd`** did not abort the path check and terminated unexpectedly when trying to access the multipath device information. The

Multipath daemon now aborts any path checks when the multipath device is removed and the problem no longer occurs.

BZ#714821

The Multipath daemon was removing a multipath device twice. This could cause multipathd to access memory already used for another purpose, and caused the multipathd daemon to terminate unexpectedly. The multipathd daemon now removes the device once and the problem no longer occurs.

BZ#719571

The kpartx utility built partition devices for invalid GUID partition tables (GPT) because it did not validate the size of GUID partitions. The kpartx utility now checks the partition size, and does not build devices for invalid GPTs.

BZ#723168

Multipath previously returned an unclear error message when it failed to find rport_id. The returned message and its severity have been adjusted.

BZ#725541

Several upstream commits have been included in the device-mapper-multipath package providing a number of bug fixes and enhancements over the previous version.

BZ#738298

Anaconda failed to recognize an existing filesystem on a zSeries Linux fibre-channel adapter (zFCP) LUN and marked it as 'Unknown' when reinstalling the system. This happened due to an incorrect setting of the DM_UDEV_DISABLE_DISK_RULES_FLAG property. Filesystem on a multipath zFCP LUN is now correctly recognized during the installation.

BZ#747604

The asynchronous TUR path checker caused multipathd to terminate unexpectedly due to memory corruption. This happened if multipathd attempted to delete a path while the asynchronous TUR checker was running on the path. The asynchronous TUR checker code has been removed, and multipathd no longer crashes on path removal.

Enhancements

BZ#636009

Multipath now supports up to 8000 device paths.

BZ#683616

To provide support for Asymmetric Logical Unit Access (ALUA), the RDAC checker has been modified to work better with devices in IOSHIP mode. The checker now sets the Task Aborted Status (TAS) bit to 1 if the TAS bit is set to 0 and changeable on a LUN (Logical Unit Number) discovery. The function now also reports PATH_UP for both the path groups in the RDAC storage in IOSHIP mode.

BZ#694602

To run multipath on IBM BladeCenter S-series with RAIDed Shared Storage Module (RSSM) demanded a manual multipath configuration to enable RSSM. Multipath now configures the server automatically.

BZ#699577

The text in the **defaults multipaths devices** sections of the **multipath.conf** man page has been improved to provide a better clarification.

BZ#713754

The **rr_min_io_rq** option has been added to the **default**, **devices**, and **multipaths** sections of the **multipath.conf** file. This option defines the number of I/O requests to route to a path before switching to the next path in the current path group. Note that the **rr_min_io** option is no longer used.

BZ#710478

UID, GID, and mode owner settings defined in **/etc/multipath.conf** for a multipath device are ignored. These access permissions are now set with the udev rules.

Users are advised to upgrade to these updated device-mapper-multipath packages, which fix these bugs and add these enhancements.

4.44.2. RHBA-2012:0502 — device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

Bug Fix

BZ#802433

Device-Mapper Multipath uses certain regular expressions in the built-in device configurations to determine a multipath device so that the correct configuration can be applied to the device. Previously, some regular expressions for the device vendor and product ID were set too broad. As a consequence, some devices could be matched with incorrect device configurations. With this update, the product and vendor regular expressions have been set more strict so that all multipath devices can now be properly configured.

All users of device-mapper-multipath are advised to upgrade to these updated packages, which fix this bug.

4.45. DEVICEKIT-POWER

4.45.1. RHEA-2011:1276 — DeviceKit-power enhancement update

Updated DeviceKit-power packages that add two enhancements are now available for Red Hat Enterprise Linux 6.

DeviceKit-power provides a daemon, API and command line tools for managing power devices attached to the system.

Enhancements

BZ#625880

To allow administrators easily disable the suspend and hibernate actions on the system, DeviceKit-power now checks the PolicyKit authorization before deciding whether an action can be completed.

BZ#727544

This update introduces a new sub-package DeviceKit-power-devel-docs, which contains developer's documentation for DeviceKit-power, so that it is now possible to install the DeviceKit-power-devel package on machines with multiple architectures without file conflicts.

All users are advised to upgrade to these updated DeviceKit-power packages, which add these enhancements.

4.46. DHCP

4.46.1. RHSA-2011:1819 — Moderate: dhcp security update

Updated dhcp packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address.

Security Fix

CVE-2011-4539

A denial of service flaw was found in the way the dhcpd daemon handled DHCP request packets when regular expression matching was used in "/etc/dhcp/dhcpd.conf". A remote attacker could use this flaw to crash dhcpd.

Users of DHCP should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, all DHCP servers will be restarted automatically.

4.46.2. RHBA-2011:1597 — dhcp bug fix and enhancement update

Updated dhcp packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. DHCPv6 is the DHCP protocol that supports IPv6 networks.

Bug Fixes

BZ#694798

Previously, when multiple DHCP clients were launched at the same time to handle multiple virtual interfaces on the same network interface card (NIC), the clients used the same seed to choose when to renew their leases. Consequently, these virtual interfaces for some clients could have been removed over time. With this update, the dhclient utility uses the Process Identifier (PID) for seeding the random number generator, which fixes the bug.

BZ#694799

If a system was rebooted while a network switch was inoperative, the network connection would recover successfully. However, it was no longer configured to use DHCP even if the dhclient utility had been running in persistent mode. With this update, the dhclient-script file has been modified to refresh the ARP (Address Resolution Protocol) table and the routing table instead of bringing the interface down, which fixes the bug.

BZ#731990

If the system included network interfaces with no hardware address, the dhcpd scan could have experienced a segmentation fault when scanning such an interface. As a consequence, the dhcpd daemon unexpectedly terminated. To prevent this issue, dhcpd now tests a pointer which represents the hardware address of the interface for the NULL value. The dhcp daemon no longer crashes.

BZ#736999

Previously, all source files were compiled with the "-fpie" or "fPIE" flag. As a consequence, the libraries used by dhcp could not have been used to build Perl modules. To fix this problem, all respective dhcp Makefiles have been modified to compile libraries with the "-fpic" or "-fPIC" flag. The libraries used by dhcp are now built without the previous restrictions.

BZ#736194

Previously, both dhcp and dhclient packages included the dhcp-options(5) and dhcp-eval(5) man pages. As a consequence, a conflict could have occurred when any of these man pages were updated, because dhcp and dhclient packages could have been upgraded separately. To prevent the problem from occurring in future updates, shared files of dhcp and dhclient packages have been moved to the dhcp-common package that is required by both dhcp and dhclient as a dependency.

Enhancements

BZ#706974

A feature has been backported from dhcp version 4.2.0. This feature allows the DHCPv6 server to be configured to identify DHCPv6 clients in accordance with their link-layer address and their network hardware type. With this update, it is now possible to define a static IPv6 address for the DHCPv6 client with a known link-layer address.

BZ#693381

Previously, the dhcpd daemon ran as root. With this update, new "-user" and "-group" options can be used with dhcpd. These options allow dhcpd to change the effective user and group ID after it starts. The dhcpd and dhcpd6 services now run the dhcpd daemon with the "-user dhcpd -group dhcpd" parameters, which means that the dhcpd daemon runs as the dhcpd user and group instead root.

Users are advised to upgrade to these updated dhcp packages, which fixes these bugs and add these enhancements.

4.47. DMIDECODE

4.47.1. RHEA-2011:1555 — dmidecode bug fix and enhancement update

An updated dmidecode package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The dmidecode package provides utilities for extracting x86 and Intel Itanium hardware information from the system BIOS or EFI (Extensible Firmware Interface), depending on the SMBIOS/DMI standard. This information typically includes system manufacturer, model name, serial number, BIOS version, and asset tag as well as other details, depending on the manufacturer. This often includes usage status for the CPU sockets, expansion slots such as AGP, PCI and ISA, among others, memory module slots, and many different kinds of I/O ports, such as serial, parallel and USB.

Prior to this update, the extended records for the DMI types Memory Device (DMI type 17) and Memory Array Mapped Address (DMI type 19) were missing from the dmidecode utility output. With this update, dmidecode has been upgraded to upstream version 2.11, which updates support for the SMBIOS specification to version 2.7.1, thus fixing this bug. Now, the dmidecode output contains the extended records for DMI type 17 and DMI type 19. (BZ#654833)

All users of dmidecode are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.48. DNSMASQ

4.48.1. RHBA-2011:1746 — dnsmasq bug fix update

An updated dnsmasq package that addresses two bugs is now available for Red Hat Enterprise Linux 6.

Dnsmasq is a lightweight and easy-to-configure DNS forwarder and DHCP server.

Bug Fixes

BZ#584009

Three changes were made to /etc/init.d/dnsmasq, the dnsmasq startup script:

- If dnsmasq was started or restarted by a non-privileged user, the startup script previously failed silently. With this update, the dnsmasq startup script now exits with a status code of 4 (user had insufficient privilege) and returns a "User has insufficient privilege" error to STD OUT when started or restarted by a non-privileged user.
- A "force-reload" option was added: The "service force-reload dnsmasq" command now forces dnsmasq to reload. Previously, it did nothing.
- If /etc/init.d/dnsmasq passed an invalid argument, previously the startup script exited with a status code of 1 (generic or unspecified error). With this update, the startup script now exits correctly, returning a status code of 2 (invalid or excess argument) in such a circumstance.

BZ#704073

If the virtual bridge interface (virbr0) was up and dnsmasq was started by default, dnsmasq could, in some circumstances, write a "DHCP packet received on eth(x) which has no address" message to /var/log/messages. Note: this message was not in error. The message was written if an actual interface (eg eth1) was up; did not have a configured IP address (eg was slaved to a logical bonded interface); and was in the same LAN as another host which generated a DHCP request. The message had little-to-no utility, however: it presented a warning where none was needed. With this update, this message is no longer written to /var/log/messages in these, and equivalent, circumstances.

All dnsmasq users should install this update which makes these changes.

4.49. DOSFSTOOLS

4.49.1. RHBA-2011:1552 — dosfstools bug fix update

An updated dosfstools package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The dosfstools package contains a set of tools for creating and maintaining FAT-type file systems. It includes the mkdosfs and dosfsck utilities, which make and check MS-DOS FAT file systems on hard drives and floppy disks.

Bug Fixes

BZ#624596

Previously, when the dosfsck and the dosfslabel utilities were executed on the IBM System z architecture using a FAT32 file system, they terminated with this error message: "Logical sector size is zero". This was caused by unaligned fields which were first byte-wise copied. With this fix, the fields are not pre-copied any more, but are accessed the same way as on the i686 architecture.

BZ#677789

The fsck.vfat utility terminated due to buffer overflow. This occurred when checking a device with the corrupted VFAT file system if there were any chains of orphaned clusters. The name of the newly created file that contained these clusters was printed directly into the name field, which led to an out of boundary write. The name is now printed into the buffer and individual parts are then correctly copied into the appropriate field.

BZ#688128

The dosfslabel utility displayed an error message when labeling the FAT32 file system due to some of its internal structures being initialized incorrectly. The dosfslabel utility now reads the FAT file system first, which fixes the problem.

BZ#709266

The mkfs.vfat utility did not correctly detect device partitions on RAID devices. As a consequence, formatting failed with an error message. This was caused by an invalid mask for the statbuf.st_rdev variable. The mask has been fixed to be at least four bytes long and the problem no longer occurs.

All users of dosfstools are advised to upgrade to this updated package, which resolves these bugs.

4.50. DOXYGEN

4.50.1. RHBA-2011:1174 — doxygen bug fix update

Updated doxygen packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Doxygen can generate an online class browser in HTML and/or a reference manual in LaTeX from a set of documented source files. The documentation is extracted directly from the sources.

Bug Fix

BZ#690076

Prior to this update, Doxygen required invalid BuildRequires on the qt-devel package. With this update, packages with BuildRequires dependencies on the qt-devel package have been fixed. Now, these packages explicitly require qt4-devel.

All users of Doxygen are advised to upgrade to these updated packages, which fix this bug.

4.51. DRACUT

4.51.1. RHBA-2012:1319 — dracut bug fix update

Updated dracut packages that fix a bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The dracut packages include an event-driven initramfs generator infrastructure based on the udev device manager. The virtual file system, initramfs, is loaded together with the kernel at boot time and initializes the system, so it can read and boot from the root partition.

Bug Fix

BZ#860350

If the "/boot/" directory was not on a separate file system, dracut called the sha512hmac utility with a file name prefixed with "/sysroot/boot". Consequently, sha512mac searched for the file checksum in "/boot/", returned errors, and dracut considered the FIPS check to have failed. Eventually, a kernel panic occurred. With this update, dracut uses a symlink linking "/boot" to "/sysroot/boot", sha512mac can now access files in "/boot/", and FIPS checks now pass, allowing the system to boot properly in the described scenario.

All users of dracut are advised to upgrade to these updated packages, which fix this bug.

4.51.2. RHBA-2011:1521 — dracut bug fix and enhancement update

Updated dracut packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The dracut packages include an event-driven initramfs generator infrastructure based on udev. The virtual file system, initramfs, is loaded together with the kernel at boot time and initializes the system, so it can read and boot from the root partition.

Bug Fixes

BZ#659076

Previously, dracut incorrectly displayed that it loaded SELinux even if SELinux was disabled in the config file and "selinux=0" was not specified on the kernel command line. As a consequence, an error message could confuse the user when booting the system. With this update, the dracut utility is modified and the error message no longer appears.

BZ#696980

Due to an error in the dracut module script, the system could fail to find the root volume if a static IP address was specified. As a consequence, the system did not boot. With this update, the error is corrected, and the system is able to boot with a static IP address.

BZ#698160

When mounting the root device over the NFS (Network File System) protocol, the /var/lib/rpcbind directory created by initramfs was world-writable. The dracut tool has been modified to generate initramfs which now sets the ownership to the rpc user and the group.

BZ#698165

When auto-assembling an md RAID device, initramfs used an invalid parameter when calling the mdadm tool. This prevented the system from booting if the root device was on the RAID device. The invalid parameter has been removed and the system now boots properly.

BZ#698215

When auto-assembling an md RAID device, an error in the mdraid_start.sh script prevented the system from booting if the root device was on the RAID device. The error in the script has been fixed and the system now boots correctly.

BZ#701309

Prior to this update, the /var/lib/nfs/prc_pipefs partition could not be accessed on system boot. The problem occurred when booting the system with NFS set as the root partition with at least one separate /var partition. This was caused by initramfs mounting the /var partition over the existing rpc_pipefs partition. The initramfs file system now mounts entries in /etc/fstab.sys, which fixes the problem.

BZ#707609

The dm-mod and dm-crypt kernel modules were missing from the list of kernel modules, which are pre-loaded for the FIPS-140 check. These modules have been added to the list with this update.

BZ#712254

When loading SELinux from inside initramfs, the output of the SELinux commands could be garbled if the user used non-Latin locales. The initramfs file system has been modified to turn off localization for the SElinux commands, which results in readable messages.

BZ#737134

The QLogic qla4xxx iSCSI driver and the iSCSI (Internet Small Computer System Interface) transport layer now support iSCSI boot from Storage Area Network (SAN) using the iscsistart. With this update, dracut is modified to support these changes.

BZ#737593

If the user installed a system with rootfs on a RAID device where RAID members were encrypted, dracut failed to assemble the RAID device on reboot. As a consequence, the system did not boot. A patch has been applied to address this issue, and the RAID device is now assembled on every boot so that the system boots successfully.

BZ#741430

When applying SELinux labels for /dev in initramfs, the restorecon tool did not alter the MCS/MLS label only types. To fix this problem, the "-F" option has been added to all calls of restorecon.

BZ#742920

Prior to this update, the boot process timed out for network settings with DHCP involved. A patch has been applied to extend the timeout interval if DHCP is involved, which fixes the problem.

Enhancements

BZ#701864

This update adds support for iSCSI (Internet Small Computer System Interface) partial offload functionality for certain Broadcom network devices.

BZ#740487

This update adds the dracut-fips-aesni subpackage. Note that the package should be installed when using the aesni-intel module in FIPS mode.

BZ#723548

This update adds support for Logical Volume Management (LVM) mirror devices to serve as root devices. Additionally degraded mirrors are used after a certain timeout if the other half cannot be found at booting time.

BZ#729573

This update adds support for configuring an interface with automatic IPv6 and DHCP over IPv4 by using the "ip=[interface]:dhcp,auto6" command line parameter.

BZ#736094

With this update, the Broadcom FCoE (Fibre Channel over Ethernet) offload driver is now supported.

Users of dracut are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.51.3. RHBA-2012:0331 — dracut bug fix update

Updated dracut packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The dracut packages include an event-driven initramfs generator infrastructure based on the udev device manager. The virtual file system, initramfs, is loaded together with the kernel at boot time and initializes the system, so it can read and boot from the root partition.

Bug Fixes

BZ#790943

When sourcing dracut modules, dracut did not check whether the "install" script for the module exists and is executable. Therefore, if the script was missing, an attempt to execute the script failed. As a consequence, dracut did not execute the "installkernel" script, and the module was not included in the initramfs image. This problem has been fixed, dracut now performs the check and only executes the "install" script when it exists. Then, the "installkernel" script is correctly executed and the module is installed in the initramfs image.

BZ#791128

Previously, dracut did not correctly handle a situation when booting a system with a degraded RAID array. In such a case, the initial RAM disk image (initramfs) was not able to start the array and the system did not boot. With this update, the initramfs forces the array to start and the system now boots as expected.

All users of dracut are advised to upgrade to these updated packages, which fix these bugs.

4.52. DUMP

4.52.1. RHBA-2011:1095 — dump bug fix update

Updated dump packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The dump package contains both "dump" and "restore" commands. The "dump" command examines files in a file system, determines which ones need to be backed up, and copies those files to a specified disk, tape, or other storage medium. The "restore" command performs the inverse function of "dump"; it can restore a full backup of a file system. Subsequent incremental backups can then be layered on top of the full backup. Single files and directory subtrees may also be restored from full or partial backups.

Bug Fixes

BZ#702593

Prior to this update, the dump utility passed wrong arguments to the "clone(2)" system call. As a result, dump became unresponsive when executed on the S/390 or IBM System z architecture. This bug has been fixed in this update so that dump now passes correct arguments and no longer hangs.

BZ#691434

Under certain circumstances, the dump utility could have failed to detect holes in files correctly. When a user attempted to restore an erroneous backup using the "restore" command, an error message "Missing blocks at end of [path], assuming hole" could have been displayed. In such case, the backup could have not been restored properly. This bug has been fixed in this update so that dump now handles holes in files as expected.

BZ#658890

Prior to this update, the "dump -w" command did not recognize ext4 file systems as supported. With this update, the bug has been fixed so that "dump -w" now recognizes the ext4 file systems as supported.

All users of dump should upgrade to these updated packages, which fix these bugs.

4.53. E2FSPROGS

4.53.1. RHBA-2011:1735 — e2fsprogs bug fix and enhancement update

Updated e2fsprogs packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The e2fsprogs packages contain a number of utilities that create, check, modify, and correct inconsistencies in ext2, ext3, and ext4 file systems. This includes e2fsck (which repairs file system inconsistencies after an unclean shutdown), mke2fs (which initializes a partition to contain an empty file system), tune2fs (which modifies file system parameters), and most of the other core file system utilities.

Bug Fixes

BZ#676465

Running the "e2fsck" command on certain corrupted file systems failed to correct all errors during the first run. This occurred when a file had its xattr block cloned as a duplicate, but the block was later removed from the file because the file system did not contain the xattr feature. However, the block was not cleared from the block bitmaps. During the second run, e2fsck found the cloned xattr block

as in use, but not owned by any file, and had to repair the block bitmaps. With this update, the processing of duplicate xattr blocks is skipped on non-xattr file systems. All problems are now discovered during the first run.

BZ#679931

On certain devices with very large physical sector size, the mke2fs utility set the block size to be as large as the size of the physical sector. In some cases, the size of the physical sector was larger than the page size. As a consequence, the file system could not be mounted and, in rare cases, the utility could even fail. With this update, the default block size is not set to be larger than the system's page size, even for large physical sector devices.

BZ#683906

Previously, multiple manual pages contained typos. These typos have been corrected with this update.

BZ#713475

This update modifies parameters of the "mke2fs" command to be consistent with the "discard" and "nodiscard" mount options for all system tools (like mount, fsck, or mkfs). The user is now also informed about the ongoing discard process.

BZ#730083

Previously, the libcomm_err libraries were built without the read-only relocation (RELRO) flag. Programs built against these libraries could be vulnerable to various attacks based on overwriting the ELF section of a program. To enhance the security, the e2fsprogs package is now provided with partial RELRO support.

Enhancements

BZ#679892

Previously, the tune2fs tool could not set "barrier=0" as the default option on the ext3 and ext4 file systems. With this update, users are now able to set this option when creating the file system, and do not have to maintain the option in the /etc/fstab file across all of the file systems and servers.

BZ#713468

Previously, raw e2image output files could be extremely large sparse files, which were difficult to copy, archive, and transport. This update adds support for exporting images in the qcow format. Images in this format are small and easy to manipulate.

Users are advised to upgrade to these updated e2fsprogs packages, which fix these bugs and add these enhancements.

4.54. EMACS

4.54.1. RHBA-2012:0042 — emacs bug fix update

Updated emacs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (elisp), and the capability to read email and news.

Bug Fix

BZ#769673

Emacs did not properly terminate if it was started remotely and the remote client session was closed while Emacs was suspended. Under these conditions, Emacs entered an infinite loop in the code and gradually consumed all available computer resources, which caused the system to become unstable. With this update, Emacs has been modified, and it now terminates correctly when the remote session is closed.

All users of emacs are advised to upgrade to these updated packages, which fix this bug.

4.54.2. RHBA-2012:0348 — emacs bug fix update

Updated emacs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (elisp), and the capability to read e-mail and news.

Bug Fix

BZ#796053

In ispell mode, Emacs used the spell checkers in the following order: Ispell, Aspell, and Hunspell. However, Ispell is no longer available and Aspell does not have any dictionaries installed by default. Consequently, because Emacs found Aspell before the default Hunspell, the spell check failed and Emacs reported the following error message:

```
ispell-init-process: Error: No word lists can be found for the language
"en_US".
```

With this update, Emacs has been modified to look for the spell checkers in the following order: Hunspell, Aspell, and Ispell. This ensures that Hunspell is used by default when it is available.

All users of emacs are advised to upgrade to these updated packages, which fix this bug.

4.55. ESC

4.55.1. RHBA-2011:1718 — esc bug fix update

An updated esc package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The esc package contains the Smart Card Manager GUI (Graphical User Interface), which allows the user to manage security smart cards. The primary function of the tool is to enroll smart cards, so that they can be used for common cryptographic operations, such as secure email and website access.

Bug Fixes

BZ#253077

If the user resized an ESC window and closed it, the window did not preserve its size when opening it again. If the user wanted the window to be larger, for example, to make it easier to read, the user had to resize the window every single time when it was opened again. A patch has been applied to address this issue and the previous window size is now restored when opening ESC.

BZ#682216

Previously, during the shut down sequence of the escd daemon, the daemon reported a failure of certain instances. ESC terminated unexpectedly with a segmentation fault as a consequence. This update modifies the daemon to exit quietly. As a result, ESC no longer terminates unexpectedly.

BZ#702683

The esc-prefs.js file contains helpful commented settings designed to assist the user in trying rarely used settings if the situation warrants. A number of these settings in the file contained typos. The typos have been corrected with this update.

BZ#704281

Previously, ESC could have terminated with a segmentation fault after the user had inserted a new smart card into the reader. This was due to a bug in the code which helped to bring a pop-up window to the foreground. The code is no longer needed to assure window focus, therefore it is no longer being executed. As a result, ESC no longer terminates in the scenario described.

All users of esc are advised to upgrade to this updated package, which fixes these bugs.

4.55.2. RHBA-2012:0472 — esc bug fix update

An updated esc package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The esc packages contain the Smart Card Manager GUI, which allows user to manage security smart cards. The primary function of the tool is to enroll smart cards, so that they can be used for common cryptographic operations, such as secure e-mail and website access.

Bug Fixes

BZ#807264

The ESC utility did not start when the latest 10 series release of the XULRunner runtime environment was installed on the system. This update includes necessary changes to ensure that ESC works as expected with the latest version of XULRunner.

BZ#807806

After removing and replacing an enrolled token, ESC could terminate unexpectedly followed by a traceback. A patch has been applied to address this issue and ESC now displays the enrolled smart card details as expected.

All users of esc are advised to upgrade to these updated packages, which fix these bugs.

4.56. EXPAT

4.56.1. RHSA-2012:0731 — Moderate: expat security update

Updated expat packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Expat is a C library written by James Clark for parsing XML documents.

Security Fixes

CVE-2012-0876

A denial of service flaw was found in the implementation of hash arrays in Expat. An attacker could use this flaw to make an application using Expat consume an excessive amount of CPU time by providing a specially-crafted XML file that triggers multiple hash function collisions. To mitigate this issue, randomization has been added to the hash function to reduce the chance of an attacker successfully causing intentional collisions.

CVE-2012-1148

A memory leak flaw was found in Expat. If an XML file processed by an application linked against Expat triggered a memory re-allocation failure, Expat failed to free the previously allocated memory. This could cause the application to exit unexpectedly or crash when all available memory is exhausted.

All Expat users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, applications using the Expat library must be restarted for the update to take effect.

4.57. FCOE-UTILS

4.57.1. RHBA-2011:1607 — fcoe-utils bug fix and enhancement update

An updated fcoe-utils package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The fcoe-utils package provides Fibre Channel over Ethernet (FCoE) utilities, such as the fcoeadm command line tool for configuring FCoE interfaces, and the fcoemon service to configure DCB Ethernet QOS filters.

The fcoe-utils package has been upgraded to upstream version 1.0.20, which provides a number of bug fixes and enhancements over the previous version. (BZ#695941)

Bug Fixes

BZ#639466

When stopping the fcoe service, the fcoe initscript did not properly clean up after itself as expected (did not remove FCoE devices, kill related processes and unload FCoE drivers). As a consequence, FCoE interfaces were not brought down and FCoE related threads were still running after the fcoe had been stopped. The "service fcoe stop" command is used to ensure safe after-update service restarts on FCoE dependent systems, therefore it cannot be used to remove FCoE devices and unload related kernel modules. Concerning this situation, the initscript has been modified to use the "stop force" command option to completely remove FCoE devices and unload related kernel modules. The fcoe service now should be stopped using the "service fcoe stop force" command.

BZ#732485

When removing a network interface with no fcoe port using the "fcoeadm -d" command, the fcoe port state machine set the removal operation incorrectly to wait without responding to fcoemon. This led to an internal error because fcoemon timed out waiting for the response. To resolve the problem, the

code has been modified to return the code for no further action under these circumstances. The "fcoeadm -d" command now works for interfaces without the fcoe port as expected.

BZ#732485

The fcoemon service did not maintain any information about the relative state of a physical network interface and its dependent VLAN interfaces. As a consequence, the fcoe port of the VLAN interface could have been out of sync with the fcoe port of the physical device, resulting in undesired behavior, such as processing link events improperly. To fix this problem, a ready flag has been introduced. This flag is set to false when the physical port is disabled. Link events are now processed correctly for the vlan ports.

BZ#732485

When answering to an FCoE Initialization Protocol (FIP) VLAN Discovery request, some switches encapsulate FIP VLAN Discovery replies in a VLAN 0 tag which is wrapped around the packet's FIP frame header. Previously, when a packet containing such a reply reached a target network interface, some devices did not remove the VLAN tag before they started to process the FIP header. If the VLAN tag was not removed, the length of the processed header was larger than was expected, therefore the FIP parsing logic was not able to parse the FIP header correctly causing a loss of the packet. With this update, the parsing logic has been modified to skip over the VLAN header when necessary, and point to the correct start of the FIP header.

BZ#743689

The timeout for a kernel reply to fcoeadm operations was set to 5 seconds, which was not enough when processing an fcoeadm operation on a system with a large number of FCoE ports while a kernel was under heavy load. As a consequence, the "internal error" message was displayed even though the operation was finished successfully. To prevent this bug, the timeout for the kernel reply was increased to 30 seconds. No error message is now sent when an fcoeadm operation succeeds.

All users of fcoe-utils are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.58. FENCE-AGENTS

4.58.1. RHBA-2011:1599 — fence-agents bug fix and enhancement update

An updated fence-agents package that fixes various bugs and adds several enhancements is now available for Red Hat Enterprise Linux 6.

Red Hat fence agents are a collection of scripts to handle remote power management for cluster devices. They allow failed or unreachable cluster nodes to be forcibly restarted and removed from the cluster.

The fence-agents package has been upgraded to upstream version 3.1.5, which provides a number of bug fixes and enhancements over the previous version. (BZ#707123)

Bug Fixes

BZ#731166

Due to a change in REST API, the fence_rhevm utility incorrectly reported status "UP" as "RUNNING". Consequently, the "fence_rhevm -o status" command always reported "OFF". This bug has been fixed, and fence_rhevm now reports status correctly.

BZ#718924

The fence_drac5 agent failed to clear its SSH sessions on exit as expected by firmware. Consequently, the fence agent appeared to be still connected to the device, and once the connection limit was reached, further logins to the device were not allowed. This bug has been fixed, and fence_drac5 now clears its SSH sessions properly.

BZ#693428

The "monitor" and "status" commands of the fence_ipmilan agent returned chassis status instead of the fence device status. As a result, when a server chassis was powered off, the fence_ipmilan agent exited with the incorrect result code "2" when passed one of these commands. Now, fence_ipmilan returns the correct result code "0" in the described scenario.

BZ#708052

When a blade server was removed from a blade chassis and was fenced via the fence_bladecenter utility with the "--missing-as-off" option enabled, and was scheduled with the "reboot" action, the fence failed. This bug has been fixed, and fence_bladecenter no longer returns an error if a blade server is missing.

BZ#718196

A list operation on fence_drac5 agents resulted in unexpected termination of fence agents. A patch has been provided to address this issue, and fence_drac5 agents now work correctly in the described scenario.

BZ#718207

When the pyOpenSSL package was not present in the system, when an error occurred, the fence_ilo agent terminated with a generic error message, making it difficult to debug the problem. Now, fence_ilo reports that a dependent package is missing in the described scenario, thus fixing this bug.

BZ#732372

The verbose mode of the fence_ipmilan agent exposed user passwords when the whole command was logged by an IPMI tool. Now, the fence_ipmilan output has been changed, and passwords remain undisclosed in the described scenario.

BZ#738384

During simultaneous unfencing operations performed via the fence_scsi agent, all nodes launched their reservation commands at the same time. Consequently, some of the commands failed. Now, fence_scsi retries to unfence a node until its reservation command succeeds.

BZ#734429

A null dereference was discovered in the fence_kdump agent, when the strchr() function returned the NULL value. With this update, the dereference has been fixed in the code and no longer occurs.

Enhancements

BZ#624673

With this update, the new fence_vmware_soap() function has been provided to enable fencing of VMware guests in ESX environments.

BZ#461948

The fence_kdump utility has been updated to integrate fencing with the kernel dump environment.

BZ#698365

With this update, the RelaxNG schema generation for fence-agents has been updated with the rha:description and rha:name attributes in its output to fence attribute group elements.

BZ#726571

The fence_ipmilan agent has been updated to support the -L option of the ipmilan daemon, thus supporting fencing with user session privileges level.

Users of fence-agents are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.58.2. RHBA-2012:0353 — fence-agents bug fix update

An updated fence-agents package that fixes one bug is now available for Red Hat Enterprise Linux 6.

Red Hat fence agents are a collection of scripts to handle remote power management for several devices. They allow failed or unreachable nodes to be forcibly restarted and removed from the cluster.

Bug Fix

BZ#785816

The fence_rhevm fencing agent uses the Red Hat Enterprise Virtualization API to check the power status ("on" or "off") of a virtual machine. In addition to the states of "up" and "down", the API includes other states like "unassigned", "powering_up", "paused", "migrating", "unknown", "not_responding", "wait_for_launch", "reboot_in_progress", "saving_state", "restoring_state", "suspended", "image_illegal", "image_locked" or "powering_down". Previously, only if the machine was in the "up" state, the "on" power status was returned. The "off" status was returned for all other states although the machine was actually running. This allowed for successful fencing even before the machine was really powered off. With this update, the fence_rhevm agent detects power status of a cluster node more conservatively, and the "off" status is returned only if the machine is really powered off, it means in the "off" state.

All users of fence-agents are advised to upgrade to this updated package, which fixes this bug.

4.58.3. RHBA-2012:0483 — fence-agents bug fix update

Updated fence-agents packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Red Hat fence agents are a collection of scripts to handle remote power management for cluster devices. They allow failed or unreachable nodes to be forcibly restarted and removed from the cluster.

Bug Fix

BZ#811873

Previously, the fence_vmware_soap fence agent did not expose the full path to a virtual machine that is required for fencing. With this update, fence_vmware_soap has been modified to support identification of virtual machines as expected.

All users of fence-agents are advised to upgrade to these updated packages, which fix this bug.

4.58.4. RHBA-2012:0548 — fence-agents bug fix update

Updated fence-agents packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Red Hat fence agents are a collection of scripts for handling remote power management for cluster devices. They allow failed or unreachable nodes to be forcibly restarted and removed from the cluster.

Bug Fix

BZ#814843

Previously, fencing a Red Hat Enterprise Linux cluster node with the fence_soap_vmware fence agent running in a virtual machine on VMWare could fail with the following error message:

```
KeyError: 'config.uuid'
```

This was because the fence agent was not able to work with more than one hundred machines in a cluster. With this update, the underlying source code has been modified to support fencing of such clusters.

All users of fence-agents are advised to upgrade to these updated packages, which fix this bug.

4.58.5. RHBA-2013:1407 — fence-agents bug fix update

Updated fence-agents packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Red Hat fence agents are a collection of scripts for handling remote power management for cluster devices. They allow failed or unreachable nodes to be forcibly restarted and removed from the cluster.

Bug Fix

BZ#1012574

Prior to this update, the fence agent for IPMI (Intelligent Platform Management Interface) could return an invalid return code when the "-M cycle" option was used. This invalid return code could cause invalid interpretation of success of a fence action, eventually causing the cluster to become unresponsive. This bug has been fixed and only predefined return codes are now returned in the described scenario.

Users of fence-agents are advised to upgrade to these updated packages, which fix this bug.

4.59. FENCE-VIRT

4.59.1. RHBA-2011:1566 — fence-virt bug fix and enhancement update

Updated fence-virt packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The fence-virt packages provide a fencing agent for virtual machines as well as a host agent which processes fencing requests.

Bug Fixes

BZ#719645

Prior to this update, the domain parameter was missing from the metadata. As a consequence, existing configurations utilizing the domain parameter did not function correctly when fencing. This update adds the domain parameter for compatibility. Now, existing configurations work as expected.

BZ#720767

Prior to this update, hash mismatches falsely returned successes for fencing. As a consequence, data corruption could occur in live-hang scenarios. This update corrects the hash handling of mismatches. Now, no more false successes are returned and the data integrity is preserved.

Enhancement

BZ#691200

With this update, the libvirt-qpid plugin now operates using QMF version 2.

All users of fence-virt are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.59.2. RHBA-2012:0485 — fence-virt bug fix update

Updated fence-virt packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The fence-virt packages provide a fencing agent for virtual machines as well as a host agent which processes fencing requests.

Bug Fix

BZ#807270

Previously, the libvirt-qpid plug-in was linked directly against Qpid libraries instead of being linked only against QMFv2 libraries. As a consequence, newer versions of Qpid libraries could not be used with the libvirt-qpid plug-in. This update modifies the appropriate makefile so that libvirt-qpid is no longer linked directly against the Qpid libraries. The libvirt-qpid plug-in does not have to be re-linked to work with the newer Qpid libraries.

All users of fence-virt are advised to upgrade to these updated packages, which fix this bug.

4.60. FILE

4.60.1. RHBA-2011:0934 — file bug fix update

Updated file packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The file command is used to identify a particular file according to the type of data contained in the file.

[Updated 7 September 2011] This update fixes a bug in which the file utility did not parse ELF (Executable and Linkable Format) binary files correctly. If an entry in the program header table contained a file offset beyond the end of file, dynamically linked files were reported as being linked statically. The file utility now recognizes files in the described scenario correctly. (BZ#730336)

Bug Fixes

BZ#676045, BZ#712992, BZ#712988

Prior to this update, the file utility could have been unable to recognize RPM files for certain supported architectures. This update improves the file type recognition, and the RPM files for all supported architectures are now correctly identified as expected.

BZ#688700

Prior to this update, the file utility did not correctly recognized the IBM System z kernel images. This problem has been corrected so that the IBM System z kernel images are now correctly recognized as expected.

BZ#692098

Prior to this update, the file utility attempted to show information related to core dumps for binary files that were not core dumps. This undesired behavior has been fixed in this update so that information related to core dumps is showed only for core dumps and not for the binary files which are not core dumps.

BZ#675691

Prior to this update, file patterns for LaTeX checked only the first 400 bytes of a file to determine the pattern type. This caused an incorrect pattern type recognition as some files could have contained a larger number of comments at the beginning of the file. Furthermore, file patterns which matched a Python script were tried before the LaTeX patterns and this undesired behavior could have caused an incorrect pattern type recognition as LaTeX files could have included a source code written in Python. With this update, the aforementioned problems have been fixed by increasing the number of first bytes checked for a LaTeX file to 4096 bytes, and by trying the LaTeX patterns before the Python patterns.

BZ#690801

Prior to this update, there were several spelling mistakes contained in the magic(5) manual page. This update corrects the spelling mistakes in the respective manual page.

BZ#716665

Prior to this update, the file utility treated MP3 files as text files, and therefore was unable to recognize the MP3 files. This undesired behavior has been fixed in this update, and the file utility now treats the MP3 files as binary files and is able to properly recognize them.

All users of file are advised to upgrade to these updated packages, which fix these bugs.

4.61. FILESYSTEM

4.61.1. RHBA-2011:0966 — filesystem bug fix update

An updated filesystem package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The filesystem package is one of the basic packages that is installed on a Red Hat Enterprise Linux system. The filesystem package contains the basic directory layout for the Linux operating system, including the correct permissions for directories.

Bug Fix

BZ#620063

Prior to this update, certain locale subdirectories in the /usr/share/locale/ directory did not have any owner set. With this update, this bug has been fixed so that the filesystem package now owns the

subdirectories of the following locales: bg_BG (Bulgarian), en_NZ (New Zealand English), fi_FI (Finnish), gl_ES (Galician), lv_LV (Latvian), ms_MY (Malaysian), sr_RS (Serbian), en@shaw (Shavian), zh_CN.GB2312 (Chinese Simplified), sr@ijekavian (Serbian Jekavian), and sr@ijekavianlatin (Serbian Jekavian Latin).

All users of filesystem are advised to upgrade to this updated package, which fixes this bug.

4.62. FIPSCHECK

4.62.1. RHEA-2011:1733 — fipscheck enhancement update

Updated fipscheck packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The fipscheck library is used to verify the integrity of modules validated under FIPS-140-2. The fipscheck package provides helper binaries for creating and verifying HMAC-SHA256 checksum files.

Enhancement

BZ#727277

Prior to this update, the fipscheck library was linked without support for read-only relocations (RELRO) flags. The updated fipscheck packages are now provided with partial RELRO support.

Users of fipscheck are advised to upgrade to these updated packages, which add this enhancement.

4.63. FIREFOX

4.63.1. RHSA-2012:0079 — Critical: firefox security update

Updated firefox packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2011-3659

A use-after-free flaw was found in the way Firefox removed nsDOMAttribute child nodes. In certain circumstances, due to the premature notification of AttributeChildRemoved, a malicious script could possibly use this flaw to cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0442

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0444

A flaw was found in the way Firefox parsed Ogg Vorbis media files. A web page containing a malicious Ogg Vorbis media file could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0449

A flaw was found in the way Firefox parsed certain Scalable Vector Graphics (SVG) image files that contained eXtensible Style Sheet Language Transformations (XSLT). A web page containing a malicious SVG image file could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-3670

The same-origin policy in Firefox treated http://example.com and http://[example.com] as interchangeable. A malicious script could possibly use this flaw to gain access to sensitive information (such as a client's IP and user e-mail address, or httpOnly cookies) that may be included in HTTP proxy error replies, generated in response to invalid URLs using square brackets.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.26:

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.26

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.26, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.63.2. RHSA-2012:0387 — Critical: firefox security and bug fix update

Updated firefox packages that fix multiple security issues and three bugs are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Firefox is an open source web browser.

Security Fixes

CVE-2012-0461, CVE-2012-0462, CVE-2012-0464

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0456, CVE-2012-0457

Two flaws were found in the way Firefox parsed certain Scalable Vector Graphics (SVG) image files. A web page containing a malicious SVG image file could cause an information leak, or cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0455

A flaw could allow a malicious site to bypass intended restrictions, possibly leading to a cross-site scripting (XSS) attack if a user were tricked into dropping a "javascript:" link onto a frame.

CVE-2012-0458

It was found that the home page could be set to a "javascript:" link. If a user were tricked into setting such a home page by dragging a link to the home button, it could cause Firefox to repeatedly crash, eventually leading to arbitrary code execution with the privileges of the user running Firefox.

CVE-2012-0459

A flaw was found in the way Firefox parsed certain web content containing "cssText". A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0460

It was found that by using the DOM fullscreen API, untrusted content could bypass the mozRequestFullscreen security protections. A web page containing malicious web content could exploit this API flaw to cause user interface spoofing.

CVE-2012-0451

A flaw was found in the way Firefox handled pages with multiple Content Security Policy (CSP) headers. This could lead to a cross-site scripting attack if used in conjunction with a website that has a header injection flaw.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.3 ESR

http://www.mozilla.org/security/known-vulnerabilities/firefoxESR.html

Bug Fixes

BZ#729632

When using the Traditional Chinese locale (zh-TW), a segmentation fault sometimes occurred when closing Firefox.

BZ#784048

Inputting any text in the Web Console (Tools -> Web Developer -> Web Console) caused Firefox to crash.

BZ#799042

The java-1.6.0-ibm-plugin and java-1.6.0-sun-plugin packages require the "/usr/lib/mozilla/plugins/" directory on 32-bit systems, and the "/usr/lib64/mozilla/plugins/" directory on 64-bit systems. These directories are created by the xulrunner package; however, they were missing from the xulrunner package provided by the RHEA-2012:0327 update. Therefore, upgrading to RHEA-2012:0327 removed those directories, causing dependency errors when attempting to install the java-1.6.0-ibm-plugin or java-1.6.0-sun-plugin package. With this update, xulrunner once again creates the plugins directory. This issue did not affect users of Red Hat Enterprise Linux 6.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.3 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.63.3. RHSA-2012:0515 — Critical: firefox security update

Updated firefox packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2011-3062

A flaw was found in Sanitiser for OpenType (OTS), used by Firefox to help prevent potential exploits in malformed OpenType fonts. A web page containing malicious content could cause Firefox to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0467, **CVE-2012-0468**, **CVE-2012-0469**

A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0470

A web page containing a malicious Scalable Vector Graphics (SVG) image file could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0472

A flaw was found in the way Firefox used its embedded Cairo library to render certain fonts. A web page containing malicious content could cause Firefox to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0478

A flaw was found in the way Firefox rendered certain images using WebGL. A web page containing malicious content could cause Firefox to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0471

A cross-site scripting (XSS) flaw was found in the way Firefox handled certain multibyte character sets. A web page containing malicious content could cause Firefox to run JavaScript code with the permissions of a different website.

CVE-2012-0473

A flaw was found in the way Firefox rendered certain graphics using WebGL. A web page containing malicious content could cause Firefox to crash.

CVE-2012-0474

A flaw in Firefox allowed the address bar to display a different website than the one the user was visiting. An attacker could use this flaw to conceal a malicious URL, possibly tricking a user into believing they are viewing a trusted site, or allowing scripts to be loaded from the attacker's site, possibly leading to cross-site scripting (XSS) attacks.

CVE-2012-0477

A flaw was found in the way Firefox decoded the ISO-2022-KR and ISO-2022-CN character sets. A web page containing malicious content could cause Firefox to run JavaScript code with the permissions of a different website.

CVE-2012-0479

A flaw was found in the way Firefox handled RSS and Atom feeds. Invalid RSS or Atom content loaded over HTTPS caused Firefox to display the address of said content in the location bar, but not the content in the main window. The previous content continued to be displayed. An attacker could use this flaw to perform phishing attacks, or trick users into thinking they are visiting the site reported by the location bar, when the page is actually content controlled by an attacker.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.4 ESR:

http://www.mozilla.org/security/known-vulnerabilities/firefoxESR.html

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Mateusz Jurczyk of the Google Security Team as the original reporter of CVE-2011-3062; Aki Helin from OUSPG as the original reporter of CVE-2012-0469; Atte Kettunen from OUSPG as the original reporter of CVE-2012-0470; wushi of team509 via iDefense as the original reporter of CVE-2012-0472; Ms2ger as the original reporter of CVE-2012-0478; Anne van Kesteren of Opera Software as the original reporter of CVE-2012-0471; Matias Juntunen as the original reporter of CVE-2012-0473; Jordi Chancel and Eddy Bordi, and Chris McGowen as the original reporters of CVE-2012-0474; Masato Kinugawa as the original reporter of CVE-2012-0477; and Jeroen van der Gun as the original reporter of CVE-2012-0479.

4.63.4. RHSA-2012:0710 — Critical: firefox security update

Updated firefox packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2011-3101, **CVE-2012-1937**, **CVE-2012-1938**, **CVE-2012-1939**, **CVE-2012-1940**, **CVE-2012-1941**, **CVE-2012-1946**, **CVE-2012-1947**

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-1944

Note: CVE-2011-3101 only affected users of certain NVIDIA display drivers with graphics cards that have hardware acceleration enabled.

It was found that the Content Security Policy (CSP) implementation in Firefox no longer blocked Firefox inline event handlers. A remote attacker could use this flaw to possibly bypass a web application's intended restrictions, if that application relied on CSP to protect against flaws such as cross-site scripting (XSS).

CVE-2012-1945

If a web server hosted HTML files that are stored on a Microsoft Windows share, or a Samba share, loading such files with Firefox could result in Windows shortcut files (.lnk) in the same share also being loaded. An attacker could use this flaw to view the contents of local files and directories on the victim's system. This issue also affected users opening HTML files from Microsoft Windows shares, or Samba shares, that are mounted on their systems.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.5 ESR:

http://www.mozilla.org/security/known-vulnerabilities/firefoxESR.html

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Ken Russell of Google as the original reporter of CVE-2011-3101; Igor Bukanov, Olli Pettay, Boris Zbarsky, and Jesse Ruderman as the original reporters of CVE-2012-1937; Jesse Ruderman, Igor Bukanov, Bill McCloskey, Christian Holler, Andrew McCreight, and Brian Bondy as the original reporters of CVE-2012-1938; Christian Holler as the original reporter of CVE-2012-1939; security researcher Abhishek Arya of Google as the original reporter of CVE-2012-1940, CVE-2012-1941, and CVE-2012-1947; security researcher Arthur Gerkis as the original reporter of CVE-2012-1946; security researcher Adam Barth as the original reporter of CVE-2012-1944; and security researcher Paul Stone as the original reporter of CVE-2012-1945.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.5 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.64. FIRSTAIDKIT

4.64.1. RHBA-2011:1709 — firstaidkit bug fix update

Updated firstaidkit packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

FirstAidKit is a tool that runs automated diagnostics of an installed system.

Bug Fixes

BZ#664876

Previously, FirstAidKit's GRUB plug-in incorrectly reported failure if GRUB was installed into the Master Boot Record (MBR). Due to the plug-in being unreliable, it has been removed from the firstaidkit package.

BZ#738563

The firstaidkit-plugin-grub package has been removed from Red Hat Enterprise Linux 6.2. As a consequence, in rare cases, the system upgrade operation may fail with unresolved dependencies if the plug-in has been installed in a previous version of Red Hat Enterprise Linux. To avoid this problem, the firstaidkit-plugin-grub package should be removed before upgrading the system. However, in most cases, the system upgrade completes as expected.

All users of firstaidkit are advised to upgrade to these updated packages, which fix these bugs.

4.65. FIRSTBOOT

4.65.1. RHBA-2011:1742 — firstboot bug fix update

An updated firstboot package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The firstboot utility runs after installation and guides the user through a series of steps that allows for easier configuration of the machine.

Bug Fixes

BZ#700283

Previously, the Traditional Chinese translation (zh_TW) of the Forward button on the welcome page was different from the action mentioned in the text, on the same page, referring to this button. This update provides the corrected translation.

BZ#700305

Previously, when running firstboot in Japanese locale and the user attempted to continue without setting up an account, an untranslated warning message appeared. With this update, the message is properly translated into Japanese.

All users of firstboot are advised to upgrade to this updated package, which fixes these bugs.

4.66. FREETYPE

4.66.1. RHSA-2012:0467 — Important: freetype security update

Updated freetype packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently.

Security Fixes

CVE-2012-1134, CVE-2012-1136, CVE-2012-1142, CVE-2012-1144

Multiple flaws were found in the way FreeType handled TrueType Font (TTF), Glyph Bitmap Distribution Format (BDF), Windows .fnt and .fon, and PostScript Type 1 fonts. If a specially-crafted font file was loaded by an application linked against FreeType, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2012-1126, CVE-2012-1127, CVE-2012-1130, CVE-2012-1131, CVE-2012-1132, CVE-2012-1137, CVE-2012-1139, CVE-2012-1140, CVE-2012-1141, CVE-2012-1143

Multiple flaws were found in the way FreeType handled fonts in various formats. If a specially-crafted font file was loaded by an application linked against FreeType, it could cause the application to crash.

Red Hat would like to thank Mateusz Jurczyk of the Google Security Team for reporting these issues.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

4.67. FUSE

4.67.1. RHBA-2011:1756 — fuse bug fix update

An updated fuse package that fixes one bug is now available in Red Hat Enterprise Linux 6.

The fuse package contains the file system in userspace utilities and libraries required for using fuse file systems.

Bug Fix

BZ#723757

Prior to this update, fusermount used an incorrect path to unmount. As a result, fusermount was unable to unmount mounted fuse file systems. This update, modifies fusermount to use the correct mount path. Now, mounted fuse file systems can be successfully unmounted with fusermount.

All users who use fuse file systems in their environment are advised to upgrade to this updated fuse package, which fixes this bug.

4.68. GCC

4.68.1. RHBA-2011:1644 — gcc bug fix and enhancement update

Updated gcc packages that fix various bugs and add three enhancements are now available for Red Hat Enterprise Linux 6.

The gcc packages include C, C++, Java, Fortran, Objective C, Objective C++, and Ada 95 GNU compilers, along with related support libraries.

Bug Fixes

BZ#696352

The previous version of GCC incorrectly assumed that processors based on the AMD's multi-core architecture code named Bulldozer support the 3DNow! instruction set. This update adapts the underlying source code to make sure that GCC no longer uses the 3DNow! instructions on these processors.

BZ#705764

On the PowerPC architecture, GCC previously passed the V2DImode vector parameters using the stack and returned them in integer registers, which does not comply with the Application Binary Interface (ABI). This update corrects this error so that GCC now passes these parameters using the AltiVec parameter registers and returns them via the AltiVec return value register.

BZ#721376

Previously, GCC did not flush all pending register saves in a Frame Description Entry (FDE) before inline assembly instructions. This may have led to various problems when the inline assembly code modified those registers. With this update, GCC has been adapted to flush pending register saves in FDE before inline assembly instructions, resolving this issue.

BZ#732802

Prior to this update, the gcov test coverage utility sometimes incorrectly counted even opening brackets, which caused it to produce inaccurate statistics. This update applies a patch that corrects this error so that gcov ignores such brackets, as expected.

BZ#732807

When processing source code that extensively used overloading (that is, with hundreds or more overloads of the same function or method), the previous version of the C++ front end consumed a large amount of memory. This negatively affected the overall compile time and the amount of used system resources. With this update, the C++ front end has been optimized to use less resources in this scenario.

Enhancements

BZ#696145

This update adds support for new "-mfsgsbase", "-mf16c", and "-mrdrnd" command line options, as well as corresponding intrinsics to the immintrin.h header file. This allows for reading FS and GS base registers, retrieving random data from the random data generator, and converting between floating point and half-precision floating-point types.

BZ#696370

GCC now supports AMD's next generation processors. These processors can now be specified on the command line via the "-march=" and "-mtune=" command line options.

BZ#696495

GCC now supports Intel's next generation processor instrinsics and instructions for reading the hardware random number generator.

All users of gcc are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.69. GDB

4.69.1. RHBA-2011:1699 — gdb bug fix and enhancement update

Updated gdb packages that fix multiple bugs and add three enhancements are now available for Red Hat Enterprise Linux 6.

The GNU Debugger (GDB) allows users to debug programs written in C, C++, and other languages by executing them in a controlled fashion and then printing out their data.

Bug Fixes

BZ#669432

Prior to this update, GDB could stop on error when trying to access the libpthread shared library before the library was relocated. Fixed GDB lets the relocations to be resolved first, making such program debuggable.

BZ#669434

The Intel Fortran Compiler records certain debug info symbols in uppercase but the gfortran compiler writes case-insensitive symbols in lowercase. As a result, GDB could terminate unexpectedly when

accessing uppercase characters in the debug information from the Intel Fortran Compiler. With this update, GDB properly implements case insensitivity and ignores the symbols case in the symbol files.

BZ#692386

When the user selected the "-statistics" option with a negative number as a result, GDB printed the minus sign twice. This has been fixed and GDB now displays negative numbers with one minus sign only.

BZ#697900

On the PowerPC and the IBM System z architectures, GDB displayed only LWP (light-weight process) identifiers which matched the Linux TID (Thread Identifier) values for the threads found in the core file. GDB has been fixed to initialize the libthread_db threads debugging library when accessing the core file. GDB now correctly displays the pthread_t identifier in addition to the LWP identifier on the aforementioned architectures.

BZ#702427

Structure field offsets above 65535 described by the DWARF DW_AT_data_member_location attribute were improperly interpreted as a 0 value. GDB has been modified and can now handle also large structures and their fields.

BZ#704010

The difference between the very closely related "ptype" and "whatis" commands was not clearly defined in the gdb info manual. Detailed differences between these commands have been described in the manual.

BZ#712117

Prior to this update, the "info sources" subcommand printed only relative paths to the source files. GDB has been modified to correctly display the full path name to the source file.

BZ#730475

Modifying a string in the executable using the "-write" command line option could fail with an error if the executable was not running. With this update, GDB can modify executables even before they are started.

Enhancements

BZ#696890

With this update, Float16 instructions on future Intel processors are now supported.

BZ#698001

Debugged programs can open many shared libraries on demand at runtime using the dlopen() function. Prior to this update, tracking shared libraries that were in use by the debugged program could lead to overhead. The debugging performance of GDB has been improved: the overhead is now lower if applications load many objects.

BZ#718141

Prior to this update, GDB did not handle DWARF 4 .debug_types data correctly. Now, GDB can correctly process data in the DWARF 4 format.

All GDB users are advised to upgrade to these updated gdb packages, which fix these bugs and add these enhancements.

4.70. GDM

4.70.1. RHBA-2012:1447 — gdm bug fix update

Updated gdm packages that fix a bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The GNOME Display Manager (GDM) is a highly configurable reimplementation of XDM, the X Display Manager. GDM allows you to log into your system with the X Window System running and supports running several different X sessions on your local machine at the same time.

Bug Fix

BZ#860645

When gdm was used to connect to a server via XDMCP (X Display Manager Control Protocol), another connection to a remote system using the "ssh -X" command resulted in wrong authorization with the X server. Consequently, applications such as xterm could not be displayed on the remote system. This update provides a compatible MIT-MAGIC-COOKIE-1 key in the described scenario, thus fixing this bug.

All users of gdm are advised to upgrade to these updated packages, which fix this bug.

4.70.2. RHBA-2011:1721 — gdm bug fix update

Updated gdm packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The GNOME Display Manager (GDM) provides the graphical login screen, shown shortly after boot up, log out, and when user-switching.

Bug Fixes

BZ#661618

GDM did not properly queue up multiple authentication messages so that messages could quickly be overwritten by newer messages. The queueing mechanism has been modified, and this problem no longer occurs.

BZ#628462

If a Russian keyboard layout was chosen during system installation, the login screen was configured to use Russian input for user names and passwords by default. However, GDM did not provide any visible way to switch between keyboard layouts, and pressing Left Shift and Right Shift keys did not cause the input to change to ASCII mode in GDM. Consequently, users were not able to log in to the system. With this update, GDM allows users to switch keyboard layout properly using the keyboard layout indicator, and users can now log in as expected.

BZ#723515

GDM did not properly release file descriptors used with XDMCP indirect queries. As a consequence, the number of file descriptors used by GDM increased with every XDMCP chooser restart, which, in some cases, led to memory exhaustion and a GDM crash. The underlying GDM code has been modified to manage file descriptors properly, and the problem no longer occurs in this scenario.

BZ#670619

In multi-monitor setups, GDM always displayed the login window on the screen that was determined as active by the mouse pointer position. This behavior caused unpredictable login window placement in dual screen setups when using the NVIDIA's TwinView Dual-Display Architecture because the mouse pointer initially appeared exactly between the monitors outside of the visible screen. GDM now uses new logic to ensure that the initial placement of the mouse pointer and the login window are consistently on one screen.

BZ#645453

The GDM simple greeter login window displayed "Suspend", "Restart" and "Shut Down" buttons even though the buttons were disabled in GDM configuration and the PolicyKit toolkit disallowed any stop, restart, suspend actions on the system. With this update, GDM logic responsible for setting up the greeter login window has been modified and these buttons are no longer displayed under these circumstances

BZ#622561

When authenticating to a system and the fingerprint authentication method was enabled, but no fingerprint reader was attached to the machine, GDM erroneously displayed authentication method buttons for a brief moment. With this update, GDM displays authentication method buttons only if the authentication method is enabled and a reading device is connected.

BZ#708430

GDM did not properly handle its message queue. Therefore, when resetting a password on user login, GDM displayed an error message from a previous unsuccessful attempt. The queueing mechanism has been modified, and this problem no longer occurs.

BZ#688158

When logging into a system using LDAP authentication, GDM did not properly handle LDAP usernames containing backslash characters. As a consequence, such usernames were not recognized and users were not able to log in even though they provided valid credentials. With this update, GDM now handles usernames with backslash characters correctly and users can log in as expected.

All users of gdm are advised to upgrade to these updated packages, which fix these bugs.

4.70.3. RHEA-2012:0435 — gdm enhancement update

Updated gdm packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The GNOME Display Manager (GDM) provides the graphical login screen, shown shortly after boot up, logout, and when user-switching.

Enhancement

BZ#799940

Previously, X server audit messages were not included by default in the X server log. Now, those messages are unconditionally included in the log. Also, with this update, verbose messages are added to the X server log if debugging is enabled in the /etc/gdm/custom.conf file (by setting "Enable=true" in the [debug] section).

All users of gdm are advised to upgrade to these updated packages, which add this enhancement.

4.71. GHOSTSCRIPT

4.71.1. RHSA-2012:0095 — Moderate: ghostscript security update

Updated ghostscript packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Ghostscript is a set of software that provides a PostScript interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files.

Security Fixes

CVE-2009-3743

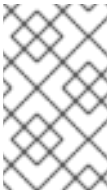
An integer overflow flaw was found in Ghostscript's TrueType bytecode interpreter. An attacker could create a specially-crafted PostScript or PDF file that, when interpreted, could cause Ghostscript to crash or, potentially, execute arbitrary code.

CVE-2010-2055

It was found that Ghostscript always tried to read Ghostscript system initialization files from the current working directory before checking other directories, even if a search path that did not contain the current working directory was specified with the "-I" option, or the "-P-" option was used (to prevent the current working directory being searched first). If a user ran Ghostscript in an attacker-controlled directory containing a system initialization file, it could cause Ghostscript to execute arbitrary PostScript code.

CVE-2010-4820

Ghostscript included the current working directory in its library search path by default. If a user ran Ghostscript without the "-P-" option in an attacker-controlled directory containing a specially-crafted PostScript library file, it could cause Ghostscript to execute arbitrary PostScript code. With this update, Ghostscript no longer searches the current working directory for library files by default.



NOTE

The fix for CVE-2010-4820 could possibly break existing configurations. To use the previous, vulnerable behavior, run Ghostscript with the "-P" option (to always search the current working directory first).

CVE-2010-4054

A flaw was found in the way Ghostscript interpreted PostScript Type 1 and PostScript Type 2 font files. An attacker could create a specially-crafted PostScript Type 1 or PostScript Type 2 font file that, when interpreted, could cause Ghostscript to crash or, potentially, execute arbitrary code.

Users of Ghostscript are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.72. GLIBC

4.72.1. RHSA-2011-1526 — Low: glibc bug fix and enhancement update

Updated glibc packages that fix two security issues, numerous bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, a Linux system cannot function properly.

Security Fixes

CVE-2009-5064

A flaw was found in the way the ldd utility identified dynamically linked libraries. If an attacker could trick a user into running ldd on a malicious binary, it could result in arbitrary code execution with the privileges of the user running ldd.

CVE-2011-1089

It was found that the glibc addmntent() function, used by various mount helper utilities, did not handle certain errors correctly when updating the mtab (mounted file systems table) file. If such utilities had the setuid bit set, a local attacker could use this flaw to corrupt the mtab file.

Red Hat would like to thank Dan Rosenberg for reporting the CVE-2011-1089 issue.

Bug Fixes

BZ#676467

The installation of the glibc-debuginfo.i686 and glibc-debuginfo.x86_64 packages failed with a transaction check error due to a conflict between the packages. This update adds the glibc-debuginfo-common package that contains debuginfo data that are common for all platforms. The package depends on the glibc-debuginfo package and the user can now install debuginfo packages for different platforms on a single machine.

BZ#676591

When a process corrupted its heap, the **`malloc()`** function could enter a deadlock while creating an error message string. As a result, the process could become unresponsive. With this update, the process uses the **`mmap()`** function to allocate memory for the error message instead of the **`malloc()`** function. The **`malloc()`** deadlock therefore no longer occurs and the process with a corrupted heap now aborts gracefully.

BZ#692838

India has adopted a new symbol for the Indian rupee leaving the currency symbol for its Unicode U20B9 outdated. The rupee symbol has been updated for all Indian locales.

BZ#694386

The **`strncmp()`** function, which compares characters of two strings, optimized for IBM POWER4 and

POWER7 architectures could return incorrect data. This happened because the function accessed the data past the zero byte (\0) of the string under certain circumstances. With this update, the function has been modified to access the string data only until the zero byte and returns correct data.

BZ#699724

The **`crypt()`** function could cause a memory leak if used with a more complex salt. The leak arose when the underlying NSS library attempted to call the dlopen() function from libnspr4.so with the RTLD_NOLOAD flag. With this update, the dlopen() with the RTLD_NOLOAD flag has been fixed and the memory leak no longer occurs.

BZ#700507

On startup, the **nscd** daemon logged the following error into the log file if SELinux was active:

```
rhel61 nscd: Can't send to audit system: USER_AVC avc:  netlink
poll: error 4#012: exe="?" sauid=28 hostname=? addr=? terminal=?
```

This happened because glibc failed to preserve the respective capabilities on UID change in the AVC thread. With this update, the AVC thread preservers the respective capabilities after the **nscd** startup.

BZ#703481, BZ#703480

When a host was temporarily unavailable, the **nscd** daemon cached an error, which did not signalize that the problem was only transient, and the request failed. With this update, the daemon caches a value signalizing that the unavailability is temporary and retries to obtain new data after a set time limit.

BZ#705465

When a module did not provide its own method for retrieving a user list of supplemental group memberships, the libc library's default method was used instead and all groups known to the module were examined to acquire the information. Consequently, applications which attempted to retrieve the information from multiple threads simultaneously, interfered with each other and received an incomplete result set. This update provides a module-specific method which prevents this interference.

BZ#706903

On machines using the Network Information Service (NIS), the **`getpwuid()`** function failed to resolve UIDs to user names when using the passwd utility in the compat mode with a big netgroup. This occurred because glibc was compiled without the -DUSE_BINDINGDIR=1 option. With this update, glibc has been compiled correctly and **`getpwuid()`** function works as expected.

BZ#711927

A debugger could have been presented with an inconsistent state after loading a library. This happened because the ld-linux program did not relocate the library before calling the debugger. With this update, the library is relocated prior to the calling of the debugger and the library is accessed successfully.

BZ#714823

The getaddrinfo() function internally uses the simpler gethostbyaddr() functions. In some cases, this could result in incorrect name canonicalization. With this update, the code has been modified and the getaddrinfo() function uses the gethostbyaddr() functions only when appropriate.

BZ#718057

The getpwent() lookups to LDAP (Lightweight Directory Access Protocol) did not return any netgroup users if the NIS (Network Information Service) domain for individual users was not defined in **`/etc/passwd`**. This happened when the nss_compat mode was set as the mode was primarily intended for use with NIS. With this update, getpwent returns LDAP netgroup users even if the users have no NIS domain defined.

BZ#730379

The **`libresolv`** library is now compiled with the stack protector enabled.

BZ#731042

The pthread_create() function failed to cancel a thread properly if setting of the real time policy failed. This occurred the because __pthread_enable_asynccancel() function as a non-leaf function did not align the stack on the 16-byte boundary as required by AMD64 ABI (Application Binary Interface). With this update, the stack alignment is preserved accros functions.

BZ#736346

When calling the **`setgroups`** function after creating threads, glibc did not cross-thread signal and supplementary group IDs were set only for the calling thread. With this update, the cross-thread signaling in the function has been introduced and supplementary group IDs are set on all involved threads as expected.

BZ#737778

The **`setlocale()`** function could fail. This happened because parameter values were parsed in the set locale. With this update, the parsing is locale-independent.

BZ#738665

A write barrier was missing in the implementation of addition to linked list of threads. This could result in the list corruption after several threads called the fork() function at the same time. The barrier has been added and the problem no longer occurs.

BZ#739184

Statically-linked binaries that call the **`gethostbyname()`** function terminated because of division by zero. This happened because the getpagesize() function required the dl_pagesize field in the dynamic linker's read-only state to be set. However, the field was not initialized when a statically linked binary loaded the dynamic linker. With this update, the getpagesize() function no longer requires a non-zero value in the dl_pagesize field and falls back to querying the value through the syscall() function if the field value is not set.

Enhancements

BZ#712248

For some queries, the pathconf() and fpathconf() functions need details about each filesystem type: mapping of its superblock magic number to various filesystem properties that cannot be queried from the kernel. This update adds support for the Lustre file system to pathconf and fpathconf.

BZ#695595

The glibc package now provides functions optimized for the Intel 6 series and Intel Xeon 5600 processors.

BZ#695963

The glibc package now supports SSE2 (Streaming SIMD Extensions 2) instructions on the **`strlen()`** function for the AMD FX processors.

BZ#711987

This update adds the f_flags field to support the **`statvfs`** output received from kernel.

BZ#738763

The Linux kernel supports the UDP **`IP_MULTICAST_ALL`** socket option, which provides the ability to turn off IP Multicast multiplexing. This update adds the option to glibc.

Users are advised to upgrade to these updated glibc packages, which contain backported patches to resolve these issues and add these enhancements.

4.72.2. RHSA-2012:0058 — Moderate: glibc security and bug fix update

Updated glibc packages that fix two security issues and three bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, a Linux system cannot function properly.

Security Fixes

CVE-2009-5029

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way the glibc library read timezone files. If a carefully-crafted timezone file was loaded by an application linked against glibc, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-4609

A denial of service flaw was found in the remote procedure call (RPC) implementation in glibc. A remote attacker able to open a large number of connections to an RPC service that is using the RPC implementation from glibc, could use this flaw to make that service use an excessive amount of CPU time.

Bug Fixes

BZ#754116

glibc had incorrect information for numeric separators and groupings for specific French, Spanish, and German locales. Therefore, applications utilizing glibc's locale support printed numbers with the wrong separators and groupings when those locales were in use. With this update, the separator and grouping information has been fixed.

BZ#766484

The RHBA-2011:1179 glibc update introduced a regression, causing glibc to incorrectly parse groups with more than 126 members, resulting in applications such as "id" failing to list all the groups a particular user was a member of. With this update, group parsing has been fixed.

BZ#769594

glibc incorrectly allocated too much memory due to a race condition within its own malloc routines. This could cause a multi-threaded application to allocate more memory than was expected. With this update, the race condition has been fixed, and malloc's behavior is now consistent with the documentation regarding the MALLOC_ARENA_TEST and MALLOC_ARENA_MAX environment variables.

Users should upgrade to these updated packages, which contain backported patches to resolve these issues.

4.72.3. RHSA-2012:0393 — Moderate: glibc security and bug fix update

Updated glibc packages that fix one security issue and three bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Security Fix

CVE-2012-0864

An integer overflow flaw was found in the implementation of the printf functions family. This could allow an attacker to bypass FORTIFY_SOURCE protections and execute arbitrary code using a format string flaw in an application, even though these protections are expected to limit the impact of such flaws to an application abort.

Bug Fixes

BZ#783999

Previously, the dynamic loader generated an incorrect ordering for initialization according to the ELF specification. This could result in incorrect ordering of DSO constructors and destructors. With this update, dependency resolution has been fixed.

BZ#795328

Previously, locking of the main malloc arena was incorrect in the retry path. This could result in a deadlock if an sbrk request failed. With this update, locking of the main arena in the retry path has been fixed. This issue was exposed by a bug fix provided in the RHSA-2012:0058 update.

BZ#799259

Calling memcpy with overlapping arguments on certain processors would generate unexpected results. While such code is a clear violation of ANSI/ISO standards, this update restores prior memcpy behavior.

All users of glibc are advised to upgrade to these updated packages, which contain patches to resolve these issues.

4.72.4. RHBA-2012:0566 — glibc bug fix update

Updated glibc packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fixes

BZ#802855

Previously, glibc looked for an error condition in the wrong location and failed to process a second response buffer in the gaih_getanswer() function. As a consequence, the getaddrinfo() function could not properly return all addresses. This update fixes an incorrect error test condition in gaih_getanswer() so that glibc now correctly parses the second response buffer. The getaddrinfo() function now correctly returns all addresses.

BZ#813859

Previously, if the nscd daemon received a CNAME (Canonical Name) record as a response to a DNS (Domain Name System) query, the cached DNS entry adopted the TTL (Time to Live) value of the underlying "A" or "AAAA" response. This caused the nscd daemon to wait for an unexpectedly long time before reloading the DNS entry. With this update, nscd uses the shortest TTL from the response as the TTL value for the entire record. DNS entries are reloaded as expected in this scenario.

All users of glibc are advised to upgrade to these updated packages, which fix these bugs.

4.73. GMP

4.73.1. RHBA-2012:0365 — gmp bug fix update

An updated gmp package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The gmp package contains GNU MP, a library for arbitrary precision arithmetic, signed integers operations, rational numbers and floating point numbers. GNU MP is designed for speed, for both small and very large operands.

Bug Fix

BZ#798771

Previously, the interface provided by the gmp library was changed. This resulted in one exported symbol being absent in Red Hat Enterprise Linux 6 (when compared to the Red Hat Enterprise Linux 5 system). In addition, the symbol could have been reported as missing under certain circumstances. To fix this problem, this update adds the missing symbol back to the library.

All users of gmp are advised to upgrade to this updated package, which fixes this bug.

4.74. GNOME-POWER-MANAGER

4.74.1. RHBA-2012:1228 — gnome-packagekit bug fix update

Updated gnome-packagekit packages that fix a bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The gnome-packagekit packages provide session applications for the PackageKit API.

Bug Fix

BZ#822946

Previously, it was possible for the user to log out of the system or shut it down while the PackageKit update tool was running and writing to the RPM database (rpmdb). Consequently, rpmdb could become damaged and inconsistent due to the unexpected termination and cause various problems with subsequent operation of the rpm, yum, and PackageKit utilities. This update modifies PackageKit to not allow shutting down the system when a transaction writing to rpmdb is active, thus fixing this bug.

Users of gnome-packagekit are advised to upgrade to these updated packages, which fix this bug.

4.74.2. RHBA-2012:0686 — gnome-power-manager bug fix update

Updated gnome-power-manager packages that fix one bug are now available for Red Hat Enterprise Linux 6.

GNOME Power Manager uses the information and facilities provided by DeviceKit-power to display icons and handle user callbacks in an interactive GNOME session.

Bug Fix

BZ#800267

After resuming the system or re-enabling the display, an icon could appear in the notification area with an erroneous tooltip that read "Session active, not inhibited, screen idle. If you see this test, your display server is broken and you should notify your distributor." and included a URL to an external web page. This error message was incorrect, had no effect on the system and could be safely ignored. In addition, linking to an external URL from the notification and status area is unwanted. To prevent this, the icon is no longer used for debugging idle problems.

All users are advised to upgrade to these updated gnome-power-manager packages, which fix this bug.

4.75. GNOME-SCREENSAVER

4.75.1. RHEA-2011:1652 — gnome-screensaver bug fix and enhancement update

An updated gnome-screensaver package that fixes various bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The gnome-screensaver package contains the GNOME project's official screen saver program. It is designed for improved integration with the GNOME desktop, including themeability, language support, and Human Interface Guidelines (HIG) compliance. It also provides screen-locking and fast user-switching from a locked screen.

Bug Fixes

BZ#648850

When the user locked the screen and the X Window System did not support the X Resize, Rotate (XRandR) or XF86VM gamma fade extensions, then the gnome-screensaver utility terminated with a segmentation fault. With this update, additional checks are made before calling the fade_setup() function, and gnome-screensaver no longer terminates.

BZ#697892

Prior to this update, the Unlock dialog box arbitrarily changed between the monitors in dual head setups, based on the position of the mouse pointer. The Unlock dialog box is now placed on a consistent monitor instead of where the mouse is located.

BZ#719023

Previously, when docking a laptop and using an external monitor, parts of the background got cut off due to incorrect logic for determining monitor dimensions. With this update, the source code is modified and the login screen is now displayed correctly.

BZ#740892

Previously, in rare cases, the screen saver entered a deadlock if monitors were removed during the fade up. The screen was locked as a consequence. This update modifies gnome-screensaver so that the screen saver responds as expected.

Enhancement

BZ#677580

Previously, there was no indicator of the keyboard layout when the screen was locked. Users who used more than one layout did not know which layout was active. Consequently, users could be forced to type the password several times. This update adds the missing keyboard layout indicator.

All users of gnome-screensaver are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.76. GNOME-SESSION

4.76.1. RHEA-2011:1654 — gnome-session bug fix and enhancement update

Updated gnome-session packages that fix a bug and add an enhancement are now available for Red Hat Enterprise Linux 6.

The gnome-session package manages the GNOME desktop session. It starts up the other core components of GNOME and handles logout and saving of the session.

Bug Fix

BZ#664516

Prior to this update, the gnome-session utility may have improperly saved desktop sessions. As a consequence, when logging in, the running applications were incorrectly collapsed from multiple workspaces into the first workspace and their initial position was not restored. This has been fixed: applications are now restored in their original workspaces and correctly positionally placed.

Enhancement

BZ#622849

Prior to this update, users were not able to manage multiple custom GNOME sessions while being logged in. Now, multiple sessions can be managed under the Options tab of System -> Preferences -> Startup Applications.

Users are advised to upgrade to these updated gnome-session packages, which resolve this bug and add this enhancement.

4.77. GNOME-SYSTEM-MONITOR

4.77.1. RHEA-2011:1612 — gnome-system-monitor enhancement update

An enhanced gnome-system-monitor package that provides an enhancement is now available for Red Hat Enterprise Linux 6.

The gnome-system-monitor package contains a tool which allows to graphically view and manipulate the running processes on the system. It also provides an overview of available resources such as CPU and memory.

Enhancement

BZ#571597

Previously, the CPU History graph could be hard to read if it displayed large numbers of CPUs. This update modifies the design: scrollbars were added for easier manipulation of the window and random color is now generated to each CPU.

Users of gnome-system-monitor are advised to upgrade to this updated package, which adds this enhancement.

4.78. GNOME-TERMINAL

4.78.1. RHBA-2011:1172 — gnome-terminal bug fix update

An updated gnome-terminal package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The gnome-terminal package contains a terminal emulator for GNOME. It supports translucent backgrounds, opening multiple terminals in a single window (tabs) and clickable URLs.

Bug Fix

BZ#655132

Previously, the regular expression used to find URLs in the text was missing a colon character. As a consequence, the URL containing a colon was not interpreted correctly. With this update, a colon character has been added to the regular expression so that the URL is now properly interpreted.

All gnome-terminal users are advised to upgrade to this updated package, which fixes this bug.

4.79. GNUTLS

4.79.1. RHSA-2012:0429 — Important: gnutls security update

Updated gnutls packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS).

Security Fixes

CVE-2012-1573

A flaw was found in the way GnuTLS decrypted malformed TLS records. This could cause a TLS/SSL client or server to crash when processing a specially-crafted TLS record from a remote TLS/SSL connection peer.

CVE-2011-4128

A boundary error was found in the gnutls_session_get_data() function. A malicious TLS/SSL server could use this flaw to crash a TLS/SSL client or, possibly, execute arbitrary code as the client, if the client passed a fixed-sized buffer to gnutls_session_get_data() before checking the real size of the session data provided by the server.

Red Hat would like to thank Matthew Hall of Mu Dynamics for reporting CVE-2012-1573.

Users of GnuTLS are advised to upgrade to these updated packages, which contain backported patches to correct these issues. For the update to take effect, all applications linked to the GnuTLS library must be restarted, or the system rebooted.

4.80. GPM

4.80.1. RHBA-2011:1092 — gpm bug fix update

Updated gpm packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The gpm packages contain a program handling mouse services on a system console device.

Bug Fix

BZ#684920

Prior to this update, it was not possible to build the gpm packages on the supported platforms if the emacs package was installed. This problem has been resolved with this update and no longer occurs.

All users of gpm are advised to upgrade to these updated packages, which fix this bug.

4.81. GPXE

4.81.1. RHBA-2011:1765 — gpxe bug fix update

Updated gpxe packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The gpxe packages provide an open source Preboot Execution Environment (PXE) implementation and bootloader. gPXE also supports additional protocols such as DNS, HTTP, iSCSI and ATA over Ethernet.

Bug Fix

BZ#743893

Prior to this update, PXE failed to boot a virtual machine which used the virtio network interface card (NIC). An upstream patch, which incorporates the latest upstream gPXE paravirtualized network adapter (virtio-net) driver and removes the legacy Etherboot virtio-net driver, has been applied to fix this problem. Now, PXE can successfully boot virtual machines that use virtio NIC.

All users of gpxe are advised to upgrade to these updated packages, which fix this bug.

4.82. GRAPHVIZ

4.82.1. RHBA-2011:0965 — graphviz bug fix update

Updated graphviz packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Graphviz is graph visualization software used to represent structural information as diagrams, abstract graphs or networks.

Bug Fixes

BZ#624658

Several links in the Graphviz Documentation Index file led to nonexistent or incorrectly named files. This update fixes these links so that their targets resolve correctly.

BZ#624690

The graphviz test suite was disabled on the PowerPC, 64-bit PowerPC and SPARC64 architectures due to unexpected terminations with segmentation faults. The test code used in the test suite did not set the TextLayout plugin correctly, which led to the crash of the test suite. This has been fixed and the test suite passes on all architectures.

BZ#640247

Prior to this update, the About dialog box displayed "<unknown>" instead of the real name of the DotEdit utility. This has been fixed and the name is now displayed correctly.

BZ#679715

When using the graphviz utility with PHP, the gv.so module did not load and displayed the following error message:

```
/usr/lib64/php/modules/gv.so' - /usr/lib64/php/modules/gv.so: undefined
symbol: zend_error_noreturn in Unknown on line 0
```

This was caused by the SWIG tool which used the zend_error_noreturn() function to build the PHP module. SWIG has been modified and the bug no longer occurs.

All users of graphviz are advised to upgrade to these updated packages, which fix these bugs.

4.83. GRUB

4.83.1. RHBA-2011:1720 — grub bug fix and enhancement update

An updated grub package that fixes three bugs and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The GRUB utility is responsible for booting the operating system kernel.

Bug Fixes

BZ#677468

Due to an error in the underlying source code, previous versions of GRUB may have failed to boot in Unified Extensible Firmware Interface (UEFI) mode. This happened, because GRUB was making UEFI calls without aligning the stack pointer to a 16-byte boundary. With this update, a patch has been applied to correct this error, and GRUB now boots in UEFI mode as expected.

BZ#736833

Prior to this update, an attempt to install GRUB on a CCISS device may have caused the grub-install utility to report the following error:

```
expr: non-numeric argument
```

When this happened, grub-install failed to install GRUB on this device, but incorrectly reported success and returned a zero exit status. This update applies a patch that ensures that GRUB can now be successfully installed on such devices.

BZ#746106

When looking for its configuration file, the previous versions of GRUB did not respect vendor-specific EFI device path. With this update, the underlying source code has been adapted to use the vendor-specific EFI-device path as expected.

Enhancements

BZ#629408

Prior to this update, the GRUB boot loader was unable to boot from boot drives that were larger than 2.2 TB. This update adds support for such devices on UEFI systems.

BZ#671355

On BIOS-based systems, previous versions of GRUB were only able to boot from first eight disk drives. This update allows GRUB to boot from up to 128 disk drives on these systems.

All users of grub are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.84. GUILE

4.84.1. RHBA-2011:0855 — guile bug fix update

An updated guile package that fixes one bug is now available for Red Hat Enterprise Linux 6.

GUILE (GNU's Ubiquitous Intelligent Language for Extension) is a library implementation of the Scheme programming language, written in C. GUILE provides a machine-independent execution platform that can be linked in as a library during the building of extensible programs.

Bug Fix

BZ#659674

Due to a problem in the build test suite, the guile package failed to build. The problem has been resolved in this update so that the guile package now builds properly.

All users of guile are advised to upgrade to this updated package, which fixes this bug.

4.85. HTTPD

4.85.1. RHSA-2012:0128 — Moderate: httpd security update

Updated httpd packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Apache HTTP Server is a popular web server.

Security Fix

CVE-2011-3639, **CVE-2011-4317**

It was discovered that the fix for CVE-2011-3368 (released via RHSA-2011:1391) did not completely address the problem. An attacker could bypass the fix and make a reverse proxy connect to an arbitrary server not directly accessible to the attacker by sending an HTTP version 0.9 request, or by using a specially-crafted URI.

CVE-2012-0053

The httpd server included the full HTTP header line in the default error page generated when receiving an excessively long or malformed header. Malicious JavaScript running in the server's domain context could use this flaw to gain access to httpOnly cookies.

CVE-2011-3607

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way httpd performed substitutions in regular expressions. An attacker able to set certain httpd settings, such as a user permitted to override the httpd configuration for a specific directory using a ".htaccess" file, could use this flaw to crash the httpd child process or, possibly, execute arbitrary code with the privileges of the "apache" user.

CVE-2012-0031

A flaw was found in the way httpd handled child process status information. A malicious program running with httpd child process privileges (such as a PHP or CGI script) could use this flaw to cause the parent httpd process to crash during httpd service shutdown.

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon will be restarted automatically.

4.85.2. RHBA-2011:1630 — httpd bug fix update

Updated httpd packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The Apache HTTP Server is a popular web server.

Bug Fixes

BZ#694939

The Apache module "mod_proxy" implements a proxy or gateway for the Apache web server. The "ProxyErrorOverride On" option did not work if used with "mod_proxy_ajp", the AJP support module for mod_proxy. Consequently when accessing a 404 URL in the "/static" context, which was proxied with AJP, the 404 page from the proxy was displayed rather than the 404 page from Apache itself. This update corrects the code and accessing 404 URLs now works as intended, via Apache, as defined in "ErrorDocument".

BZ#700074

When a backend server sends data via SSL, and is using chunked transfer encoding, the backend splits the chunk between two different SSL blocks. Prior to this update, when transferring data via SSL through a reverse proxy implemented with Apache, "mod_proxy", and "mod_ssl", the end of the first SSL block was sometimes lost and the length of the next chunk was thus invalid. Consequently, files were sometimes corrupted during transfer via SSL. This updates implements a backported fix to this problem and the error no longer occurs.

BZ#700075

The "FilterProvider" directive of the "mod_filter" module was unable to match against non-standard HTTP response headers. Consequently, output content data was not filtered or processed as expected by httpd in certain configurations. With this update, a backported patch has been applied to address this issue, and the FilterProvider directive is now able to match against non-standard HTTP response headers as expected.

BZ#700393

In situations where httpd could not allocate memory, httpd sometimes terminated unexpectedly with a segmentation fault rather than terminating the process with an error message. With this update, a patch has been applied to correct this issue and httpd no longer crashes in the scenario described.

BZ#714704

Server Name Indication (SNI) sends the name of the virtual domain as part of the TLS negotiation. Prior to this enhancement, if a client sent the wrong SNI data the client would be rejected. With this update, in configurations where SNI is not required, "mod_ssl" can ignore the SNI hostname "hint".

BZ# 720980

Prior to this update, httpd terminated unexpectedly on startup with a segmentation fault when proxy client certificates were shared across multiple virtual hosts (using the SSLProxyMachineCertificateFile directive). With this update a patch has been applied and httpd no longer crashes in the scenario described.

BZ#729585

When the "SSLCryptoDevice" config variable in "ssl.conf" was set to an unknown or invalid value, the

httpd daemon would terminate unexpectedly with a segmentation fault at startup. With this update the code has been corrected, httpd no longer crashes, and httpd will issue an appropriate error message in this scenario.

BZ#737960

If using mod_proxy_ftp, an httpd process could terminated unexpectedly with a segmentation fault when tests were made on an IPv6 localhost enabled machine. This update implements improvements to the code and the mod_proxy_ftp process no longer crashes in the scenario described.

BZ#740242

When using the "mod_cache" module, by default, the "CacheMaxExpire" directive is only applied to responses which do not specify their expiry date. Previously, it was not possible to limit the maximum expiry time for all resources. This update applies a patch which adapts the mod_cache module to provide support for "hard" as a second argument of the CacheMaxExpire directive, allowing a maximum expiry time to be enforced for all resources.

BZ#676634

The "mod_reqtimeout" module, when enabled, allows fine-grained timeouts to be applied during request parsing. The mod_reqtimeout module has been backported from upstream in this update.

All users of httpd are advised to upgrade to these updated packages, which fix these bugs.

4.86. HWDATA

4.86.1. RHEA-2011:1663 — hwdata enhancement update

An updated hwdata package that adds various enhancements is now available for Red Hat Enterprise Linux 6.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

Enhancements

BZ#682399

The pci.ids database has been updated with information about HP Laptop WiFi chipsets.

BZ#695798

The pci.ids database has been updated with information about future Intel PCH (Platform Controller Hub) devices.

BZ#712177

The pci.ids database has been updated with correct information about QLogic IBA7322 InfiniBand devices.

BZ#713070

The pci.ids database has been updated with information about future Atheros wireless devices.

BZ#739376

The pci.ids database has been updated with information about future Broadcom wireless devices.

BZ#728909

The pci.ids database has been updated according to the latest upstream changes.

Users of hwdata are advised to upgrade to this updated package, which adds these enhancements.

4.87. IBUS

4.87.1. RHBA-2011:1645 — ibus bug fix update

Updated ibus packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

The Intelligent Input Bus for Linux OS (IBus) is an input framework for Linux OS.

Bug Fix

BZ#667031

IBus did not work on a minimal installation of Red Hat Enterprise Linux 6 if no desktop environment, such as KDE or GNOME, was installed. This issue was caused by the missing dbus-x11 package, which IBus is dependent on. The dbus-x11 package is now included as a prerequisite for IBus in the IBus spec file, and IBus now works as expected.

All users of ibus are advised to upgrade to these updated packages, which resolve this issue.

4.88. IBUS-ANTHY

4.88.1. RHBA-2011:1208 — ibus-anthy bug fix update

An updated ibus-anthy package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The ibus-anthy package contains the Anthy engine, which provides an input method for Japanese based on the IBus (Intelligent Input Bus) platform.

Bug Fix

BZ#661597

Previously, when changing the Candidate Window Page Size setting of Other under the General tab, the im-chooser application had to be restarted for the changes to take effect. This problem has been fixed and the changes made to Candidate Window Page Size now apply immediately.

All users of ibus-anthy are advised to upgrade to this updated package, which resolves this bug.

4.89. IBUS-TABLE-ERBI

4.89.1. RHBA-2011:1274 — ibus-table-erbi bug fix update

An updated ibus-table-erbi package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The ibus-table-erbi provides the Simplified Chinese input method, ErBi.

Bug Fixes

BZ#712805

Prior to this update, the ibus-table-erbi spec file contained a redundant line which printed the debug message "/usr/share/ibus-table/tables" at the end of installation. The line indicated the working directory of the post-install script and has been removed to fix the problem.

BZ#729906

Previously, the table index was updated when running the post-install script of the ibus-table-erbi package. This modified the size of the files, the MD5 Message-Digest Algorithm checksum and the access time of database files. As a consequence, the "rpm -V" command failed with false positive warnings of the aforementioned changes due to the changes not matching the values in the package metadata. This has been fixed: files that are expected to be modified when running the post-install script are now specified with correct verify flags in the spec file.

All users of ibus-table-erbi are advised to upgrade to this updated package, which resolves these bugs.

4.90. ICEDTEA-WEB

4.90.1. RHBA-2011:1624 — icedtea-web enhancement update

An updated icedtea-web package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

IcedTea-Web provides a Java web browser plug-in, a Java Web Start implementation, and the IcedTea Web Control Panel.

The icedtea-web package has been upgraded to upstream version 1.1.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#713514)

Bug Fixes

BZ#683479

The Java Web Start window invoked by the "javaws -about" command contained out-of-date information and could not be closed correctly. The information was out-dated because the Java Network Launching Protocol (JNLP) XML file defined inadequate access permissions to access the about.jnlp file, which contained the update information. With this update, the about information has been moved to an accessible location. The window failed to close as the respective process thread became unresponsive. Now, the window contains up-to-date information and the thread closes correctly.

BZ#718693

MindTerm SSH Applet failed to work as it was using class netscape.security.PrivilegeManager, which was not present in icedtea-web. This update adds the class and the applet works as expected.

BZ#731345, BZ#731358

Java Web Start and IcedTea plug-in sometimes failed to run as they were calling a java binary with a JDK-based path instead of a JRE-based path. With this update, the package spec file contains the correct definition of the path construction and javaws and icedtea-plugin call the correct java binary.

BZ#734081

When running an application with javaws, javaws failed to use the proxy settings from Firefox even though the respective setting was enabled ("Use browser settings") and failed over to the "DIRECT"

mode. This happened because javaws was looking for the DEFAULT profile in the Firefox configuration file to acquire the current proxy settings. If it failed to locate the section with the DEFAULT profile, the default "DIRECT" mode was applied. With this update, javaws uses the settings from the last section under these circumstances.

BZ#741796

Starting from version 10, Elluminate did not work with IcedTea-Web. This happened because Elluminate specified Class-Path elements in its manifest file which caused a conflict with the jnlp-specified JARs. With this update, the IcedTea-Web plug-in no longer honors the Class-Path elements (just as the Oracle implementation) and Elluminate works with IcedTea-Web as expected.

All users of icedtea-web are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.90.2. RHBA-2012:0372 — icedtea-web bug fix update

An updated icedtea-web package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The icedtea-web package provides a Java web browser plug-in, a Java Web Start implementation, and the IcedTea Web Control Panel.

The icedtea-web package has been upgraded to upstream version 1.1.5, which ensures that Firefox 10 and later does not terminate unexpectedly when LiveConnect is heavily used, and that Chrome browser tabs no longer terminate unexpectedly during JavaScript execution. (BZ#800276)

NOTE

This update is not compatible with Firefox 3.6 and earlier. If you are using such a Firefox version, upgrade to a later supported version before applying this update.

All users of icedtea-web are advised to upgrade to this updated package, which fixes these bugs.

4.91. ICU

4.91.1. RHSA-2011:1815 — Moderate: icu security update

Updated icu packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The International Components for Unicode (ICU) library provides robust and full-featured Unicode services.

Security Fix

CVE-2011-4599

A stack-based buffer overflow flaw was found in the way ICU performed variant canonicalization for some locale identifiers. If a specially-crafted locale representation was opened in an application linked against ICU, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

All users of ICU should upgrade to these updated packages, which contain a backported patch to resolve this issue. All applications linked against ICU must be restarted for this update to take effect.

4.92. IMAGEMAGICK

4.92.1. RHSA-2012:0544 — Moderate: ImageMagick security update

Updated ImageMagick packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

ImageMagick is an image display and manipulation tool for the X Window System that can read and write multiple image formats.

Security Fix

CVE-2012-0247

A flaw was found in the way ImageMagick processed images with malformed Exchangeable image file format (Exif) metadata. An attacker could create a specially-crafted image file that, when opened by a victim, would cause ImageMagick to crash or, potentially, execute arbitrary code.

CVE-2012-0248

A denial of service flaw was found in the way ImageMagick processed images with malformed Exif metadata. An attacker could create a specially-crafted image file that, when opened by a victim, could cause ImageMagick to enter an infinite loop.

CVE-2010-4167

It was found that ImageMagick utilities tried to load ImageMagick configuration files from the current working directory. If a user ran an ImageMagick utility in an attacker-controlled directory containing a specially-crafted ImageMagick configuration file, it could cause the utility to execute arbitrary code.

CVE-2012-0259

An integer overflow flaw was found in the way ImageMagick processed certain Exif tags with a large components count. An attacker could create a specially-crafted image file that, when opened by a victim, could cause ImageMagick to access invalid memory and crash.

CVE-2012-0260

A denial of service flaw was found in the way ImageMagick decoded certain JPEG images. A remote attacker could provide a JPEG image with specially-crafted sequences of RST0 up to RST7 restart markers (used to indicate the input stream to be corrupted), which once processed by ImageMagick, would cause it to consume excessive amounts of memory and CPU time.

CVE-2012-1798

An out-of-bounds buffer read flaw was found in the way ImageMagick processed certain TIFF image files. A remote attacker could provide a TIFF image with a specially-crafted Exif IFD value (the set of tags for recording Exif-specific attribute information), which once opened by ImageMagick, would cause it to crash.

Red Hat would like to thank CERT-FI for reporting CVE-2012-0259, CVE-2012-0260, and CVE-2012-1798. CERT-FI acknowledges Aleksis Kauppinen, Joonas Kuorilehto, Tuomas Parttimaa and Lasse Ylivainio of Codenomicon's CROSS project as the original reporters.

Users of ImageMagick are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of ImageMagick must be restarted for this update to take effect.

4.93. INITSCRIPTS

4.93.1. RHBA-2011:1528 — initscripts bug fix and enhancement update

An updated initscripts package that fixes number of bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The initscripts package contains system scripts to boot the system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

Bug Fixes

BZ#743222

Previously, the **restorecon** utility did not change MLS (multi-level security) levels unless the **-F** parameter was used. As a consequence, the **/dev** and **/dev/pts** filesystems were not correctly labelled after boot in systems with configured MLS policy. This bug has been fixed and the **restorecon -F** command is now used for **/dev** and **/dev/pts** by default.

BZ#734987

When an explicit configuration option, such as **crashkernel=128M**, was specified to reserve crash dump memory, the **kexec-disable** upstart job unconditionally freed up the memory if the **kdump** mechanism was not enabled. This action could not be reverted until a reboot. With this update, **kexec-disable** job has been changed to not free reserved memory, unless the **crashkernel** parameter is set to **auto**, thus fixing this bug.

BZ#675079

Previously, when the **/etc/modprobe.d/bonding.conf** file or the **modprobe.conf** file was used to set the bonding options, the bond0 interface never came up after a service restart because the **arp_ip_target** module was not restored. This bug has been fixed and **arp_ip_target** is now restored when configured in one of these files.

BZ#698520

Previously, there was a bug in the **rc.sysinit** script that allowed to properly set a hostname when more than one IP address was passed to the **ipcalc** utility. Even though it was difficult to emulate such a scenario, the **rc.sysinit** script has been fixed to prevent this bug, and **ipcalc** is now always passed only a single IP address.

BZ#700184

When a network interface was configured with the **NetworkManager** utility to statically assign an IP address or a prefix, then **NetworkManager** was stopped, and the interface was reset via the **ifdown** and **ifup** utilities, the interface lost its IP address. With this update, the network scripts have been fixed to properly read the **IPADDR0** parameter in interface configuration files, and now IP addresses of such interfaces are preserved in the described scenario.

BZ#703475

Previously, when two VLAN interfaces were bonded together, the **/etc/init.d/network** script got into a loop and became unresponsive, trying to resolve MAC addresses of the interfaces. As a result, the server was prevented from completing its start-up sequence. With this update, **/etc/init.d/network** has been fixed, MAC addresses of VLAN interfaces are now resolved properly, and bonds between such interfaces now work as expected.

BZ#705367

Previously, when the **PREFIX** option was specified for the **ifcfg** utility while the **NETMASK** option was undefined, the netmask was calculated without regard to the **PREFIX** value. With this update, the **expand_config()** function has been fixed to use the **PREFIX** properly, and the netmask is now calculated correctly in the described scenario.

BZ#702814

When a system needed to be restarted after an unexpected termination, root password was not accepted to run the emergency shell. With this update, the **rc.sysinit** script has been fixed to run the **/bin/plymouth** command instead of **/usr/bin/plymouth**, thus fixing this bug. Additionally, other relevant scripts have been updated to properly work with the separated **/usr/** directory.

BZ#703210

Due to a bug in the **/etc/init.d/halt** script, no mount point set up with the word **nfs** in its path could be unmounted at reboot or shut down. This bug has been fixed and such mount points are now unmounted properly.

BZ#681357

In Red Hat Entreprise Linux 6, when the **emergency** parameter was appended to the kernel command line, the system failed to invoke the sulogin command. With this update, the **rcS-emergency** task, which is run before the **rc.sysinit** script if **emergency** is passed to the kernel, has been added, and sulogin is now properly invoked in the described scenario.

BZ#729359

Due to a bug in the **/etc/sysconfig/network-scripts/ifdown-eth** script, the PID file name passed to the **dhclient** utility during a shutdown procedure did not include the IP version prefix. Consequently, leases for IPv6 addresses could not be released. This bug has been fixed and the shut down procedure now works properly both with the IPv4 and IPv6 clients.

Enhancements

BZ#692240

Previously, the **ifup** and **ifdown** scripts explicitly ignored IPv6 configuration files that contained an alias. With this update, clients properly utilize aliases on IPv6 devices in Red Hat Enterprise Linux.

BZ#653630, BZ#672202

There was a need to have a simple mechanism for troubleshooting network problems, integrated into existing log monitoring facilities. With this update, network scripts have been updated to report errors via the **syslog** utility, and the error messages now appear in configured **syslog** channels.

BZ#680527

Previously, configuration options for the **sysctl** utility could only be changed in the **/etc/sysctl.conf** file. With this update, several scripts have been updated to also recognize additional configuration files located in the **/etc/sysctl.d/** directory.

BZ#692410

With this update, network start-up scripts have been enhanced to support all **ethtool** command options. These options can be set via the **ETHTOOL_OPTS** parameter in configuration files located in the **/etc/sysconfig/network-scripts/** directory and take effect after reboot.

BZ#696788

With this update, start-up network scripts have been enhanced to set up static ARP (Address Resolution Protocol) entries located in the **/etc/ethers** file, allowing to load these entries early in the system startup.

Users of initscripts are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.93.2. RHBA-2012:0355 — initscripts bug fix update

An updated initscripts package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The initscripts package contains basic system scripts to boot the system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

Bug Fix

BZ#789056

The previous version of initscripts did not support IPv6 routing in the same way as IPv4 routing. IPv6 addressing and routing could be achieved only by specifying the "ip" commands explicitly with the "-6" flag in the "/etc/sysconfig/network-scripts/rule-DEVICE_NAME" configuration file (where "DEVICE_NAME" is a name of the respective network interface). With this update, related network scripts have been modified to provide support for IPv6-based policy routing. IPv6 routing is now configured separately in the the "/etc/sysconfig/network-scripts/rule6-DEVICE_NAME" configuration file.

All users of initscripts are advised to upgrade to this updated package, which fixes this bug.

4.94. IPA

4.94.1. RHSA-2011:1533 — Moderate: ipa security and bug fix update

An updated ipa package that fixes one security issue and several bugs is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE link associated with the description below.

Red Hat Identity Management is a centralized authentication, identity management and authorization solution for both traditional and cloud based enterprise environments. It integrates components of the Red Hat Directory Server, MIT Kerberos, Red Hat Certificate System, NTP and DNS. It provides web

browser and command-line interfaces. Its administration tools allow an administrator to quickly install, set up, and administer a group of domain controllers to meet the authentication and identity management requirements of large scale Linux and UNIX deployments.

Security Fix

CVE-2011-3636

A Cross-Site Request Forgery (CSRF) flaw was found in Red Hat Identity Management. If a remote attacker could trick a user, who was logged into the management web interface, into visiting a specially-crafted URL, the attacker could perform Red Hat Identity Management configuration changes with the privileges of the logged in user.

Due to the changes required to fix CVE-2011-3636, client tools will need to be updated for client systems to communicate with updated Red Hat Identity Management servers. New client systems will need to have the updated ipa-client package installed to be enrolled. Already enrolled client systems will need to have the updated certmonger package installed to be able to renew their system certificate. Note that system certificates are valid for two years by default.

Updated ipa-client and certmonger packages for Red Hat Enterprise Linux 6 were released as part of Red Hat Enterprise Linux 6.2. Future updates will provide updated packages for Red Hat Enterprise Linux 5.

Bug Fixes

BZ#705800

When installation of Identity Management clients failed, the debugging information shown in the **`/var/log/ipaclient-install.log`** file did not provide enough information to determine the cause of the failure. With this update, the **`/var/log/ipaclient-install.log`** file contains improved debugging messages that make it easier to debug a possible installation failure.

BZ#705794

The Identity Management services were not started after a reboot when the server was installed with the **`ipa-replica-install`** command. With this update, after an installation of a replica with **`ipa-replica-install`**, the **`ipa`** service is enabled using the **chkconfig** utility so that the Identity Management services are started and available after a reboot.

BZ#704012

Prior to this update, installing an Identity Management replica in a new IP subnet with an Identity Management-controlled DNS server failed. With this update, such operation no longer fails, although, the **`bind`** service needs to be restarted when a new reverse zone is added over LDAP.

BZ#703869

Previously, Identity Management replication installations were missing configuration for managed entries. As a consequence, user-private groups and netgroups were not created for host groups if they were created on the replica. This update adds the missing configuration, and user and host group creation work as expected.

BZ#723662

Prior to this update, GSSAPI credential delegation was disabled in the curl utility due to a security issue. As a result, applications that rely on delegation did not work properly. This update utilizes a new constructor argument in the xmlrpc-c client API to set the new **`CURLOPT_GSSAPI_DELEGATION`**

curl option. This option enables the credential delegation, thus fixing this bug.

BZ#698421

An Identity Management replica would occasionally fail to install while trying to initialize replication with the remote Identity Management server. With this update, the **`memberOf`** attribute is rebuilt during installation, thus fixing this issue. Note that the 389 Directory Server (**389-ds**) may crash if it is restarted while this task is running. Wait for this task to complete before requesting a restart.

BZ#743253

For NIS compatibility reasons, when a host group is created, a net group with the same name is created as well. However, when a host group is created, it was not checked whether there was a net group with the same name already existent. As a consequence, the host group was created, but the net group could not be created and the user was not notified of this. With this update, when a new host group is created, the Identity Management server checks whether a net group with the specified name exists already. If there is such a group, the operation is denied.

BZ#743936

Prior to this update, the Identity Management web user interface loaded the entire Identity Management API name space when it was being started. As a result, JSON requests returned large amount of data, which caused certain browsers to report the **`script stack space quota is exhausted`** message and prevent a user from accessing the Web UI. This update split the Web UI initialization to several smaller calls. Browsers no longer report errors and the Web UI works as expected.

BZ#719656

Running the **`ipa-nis-manage`** command disabled the NIS listener and also removed the netgroup compatibility suffix. If NIS was disabled, the automatic creation of net groups was disabled as well. Thus, creating a host group would fail to automatically create a net group. With this update, disabling NIS has no effect on the automatic creation of net groups when host groups are created.

BZ#725433

Adding an indirect automount map to a mount point that already exists returned an error, but created the map anyway. As a result, the map could not be removed with Identity Management tools. With this update, the addition of an indirect map requires the creation of a key to store the mount point. If the addition of a map fails because the key already exists, the map is removed.

BZ#744264

Prior to this update, the Web UI Password Policy interface was missing some of the password policy fields that are present in the command line version (specifically, Max failures, Failure reset interval, Lockout duration, and Priority). As a result, users could not set these parameters via the Web UI and had to use the CLI version. This update adds all the missing Password Policy fields to the Web UI.

BZ#696193

When an Identity Management server A was using a KDC on Identity Management server B, and server B does down, on server A it looked as if server B was still operational. This caused clients to fail to enroll. With this update, the underlying source code has been modified to address this issue, and client enrollment works as expected.

BZ#742327

Permission objects related to DNS were improperly formatted and added before the relevant DNS privileges (that they were members of) were added to LDAP. DNS related permissions contain just

limited information. Additionally, the privilege objects, which they were members of, lacked **memberof** LDAP attributes pointing back to the permissions. Thus, a user could get an incorrect list of permissions that were members of a DNS related privilege. With this update, permission objects formatting has been fixed and the missing **memberof** LDAP attributes in the relevant DNS privileges are properly added. Users now get a valid list of permissions (containing all the needed information) when displaying a DNS related privilege.

BZ#691531

A certificate not signed by the Identity Management Certificate Authority (CA) imported into Identity Management could not be managed by Identity Management. Performing any operations on a service or a host that would cause Identity Management to attempt to revoke a certificate would fail (for example, disabling or deleting a host or service). With this update, certificates issued by other CAs cannot be imported into an Identity Management host or a service record. Disabling and deleting hosts and services works as expected and correctly revokes certificates.

BZ#741808

An LDAP object migrated using the **migrate-ds** command could contain a multi-valued RDN attribute. However, the **migrate-ds** process picked only the first value of the RDN attribute and did not respect the value that was present in the DN in the migrated LDAP object. With this update, the value that is used in the original LDAP object DN is used, rather than the first value of a multi-valued RDN. As a result, LDAP objects with a multi-valued RDN attribute are migrated without any errors.

BZ#741677

When the **ipa-client-install** was run with the **--password** option containing a bulk password for client enrollment, the password could be printed to Identity Management client install log in a plain-text format. This behavior has been fixed, and passwords are no longer logged in the install log file.

BZ#726943

By default, the Identity Management Web UI adds a redirect from the web root to **/ipa/ui**. This makes it look like no other web resources may be used. With this update, during the installation process, the **--no-ui-redirect** option can be used to disable the default Rewrite rule. This may also be commented out manually in the **/etc/httpd/conf.d/ipa-rewrite.conf**. As a result, the web server root can point to any specified place. However, **/ipa** must remain available to Identity Management.

BZ#745957

The Identity Management Web UI did not take into account when a non-admin user was a member of an administrative role, which has more privileges than just performing self-service actions. With this update, non-admin users with an administrative role are shown the full administrative tabset as expected.

BZ#746056

Identity Management Web UI did not allow addition of an external user (that is, user that is not managed by Identity Management) as a RunAs user for a Sudo rule. An external RunAs user could be added to a Sudo rule via the command line only. With this update, adding an external user as a RunAs user is possible in the Web UI.

BZ#726123

The **automountkey-del** command includes a **--continue** option which has no function and does not affect anything. With this update, the **--continue** has been hidden, and will be deprecated in the next major release.

BZ#723622

Prior to this update, the **ipa-getkeytab** command failed with Bind errors. If 32-bit packages were used on a 64-bit system, the 32-bit cyrus-sasl-gssapi package was required. This update adds architecture-specific **Requires** to the RPM spec file, and retrieving of keytabs no longer fails.

BZ#707009

Installing an Identity Management server signed by an external CA fails with the following error:

```
cannot concatenate 'str' and 'NoneType' objects
```

This was because the required information was not being passed so the installation failed when constructing the Kerberos principal name for the Dogtag 389-ds instance. This information is now provided by the installer, thus fixing this issue.

BZ#727282

In the Identity Management Web GUI, attempting to view a certificate of a host returned the unknown command u'show' error message. Users could only use the command-line to view host certificates. The certificate buttons including Get, View, Revoke, and Restore for hosts and services have been fixed to use the correct entity name, and viewing of certificates in the Web UI works as expected.

BZ#726526

The number of ports that needed to be open between Identity Management replicas was too high. Managing such a number of ports required planning because new rules were needed for each replication agreement. With this update, Dogtag is now proxied via the existing Apache web server on ports 80 and 443, which already need to be open. Ports 944[3-6] no longer need to be open in the firewall.

BZ#727921

It is possible to add a host group as a member of a net group; however, that relationship did not appear when viewing a host group. With this update, net group membership is displayed when viewing a host group.

BZ#726715

When importing automaster maps, the **auto.direct** mount mounted on **/-** was ignored because it was considered a duplicate. Consequently, direct maps needed to be added manually. This update adds an exception for the auto.direct map when importing so that its keys can be added, and importing direct maps works as expected.

BZ#728118

The output of adding or showing a sudo rule with a runAsGroup included a reference to a **ipasudorunasgroup_group** attribute, making the output unclear. A proper label was added for runAsGroup and the sudo option, which makes the output more understandable.

BZ#728614

Using the **ipa-replica-install** did not ensure that the **dbus** service was running. Consequently, tracking certificates with **certmonger** returned an error and the installation failed. With this update, prior to starting **certmonger**, it is checked whether the dbus-daemon is running.

BZ#733436

The Identity Management server installer and **ipactl** use two different methods to determine whether Identity Management is configured. If the Identity Management uninstallation was not complete, **ipactl** may have claimed that the Identity Management server is not configured while the Identity Management server installer refused to continue because Identity Management was configured. With this update, a common function that checks whether the Identity Management server is configured has been added. During the uninstallation process of the Identity Management server, checks are run that report left-over files so that users can manually resolve these.

BZ#714238

Prior to this update, the error message returned when setting an integer value that was too large on 64-bit systems was confusing. This update limits the integer values to 2147483647 on all platforms, making error messages consistent on 32 and 64-bit systems.

BZ#729245

Adding an option to a sudo rule with the **sudurole-add-option** command did not display a summary after the option was added. With this update, a summary is printed in the form of **Added option 'x' to Sudo Rule 'y'**.

BZ#730436

Under rare circumstances, certain operations may have caused the 389 Directory Server (389-ds) to crash or not function properly. This was because NSPR (Netscape Portable Runtime) read/write locks used by 389-ds were not re-entrant. These locks were replaced with POSIX thread read-write locks in the Identity Management 389-ds plugins, and the aforementioned crashes no longer occur.

BZ#729246

Removing an option from a sudo rule with the **sudurole-remove-option** command did not display a summary after the option was removed. With this update, a summary is printed in the form of **Removed option 'x' to Sudo Rule 'y'**.

BZ#729377

Installing an Identity Management server using the **--no-host-dns** option without a DNS resolvable host name caused the installation to fail with DNS errors. This update moves the no-host-dns test so that it is tested before any DNS lookups occur, and installations with the **--no-host-dns** option do not perform any DNS validation.

BZ#732468

When Identity Management client A/PTR DNS records did not match, the **ipa-getkeytab** and **ipa-join** commands did not operate properly, and the client could not be enrolled to the Identity Management server. As a result, client installations failed every time. With this update, matching client A/PTR DNS records are no longer a requirement for **ipa-getkeytab** and **ipa-join**, and client installations succeed even when the aforementioned records do not match.

BZ#730713

Selecting a check box for users, groups, hosts, or host groups when deleting a list of objects in an HBAC rule in the Identity Management Web UI left the check box checked even when the operation

was complete and the entry was re-edited. With this update, the selection is cleared when the page is refreshed.

BZ#730751

When editing an HBAC rule in the Identity Management Web UI, the delete button was enabled even when no selection was made. This update disables the delete button when nothing is selected.

BZ#729089

Removing an external host value by checking the **update dns** check box rendered the action successful even though the host was not removed. With this update, the host is removed successfully in the aforementioned scenario.

BZ#728950

If an 389-ds certificate expired, the Identity Management services did not start .This update adds new options for 389-ds which allow to control how 389-ds reacts to an expired certificate. The default setting is to warn the user and start the services.

BZ#729665

Checking/unchecking the **Hide already enrolled** check box when adding/removing members from a group had no effect. This update removes this check box.

BZ#726725

Passing an empty map name to the **automountmap** or **automountkey** command returned the following error:

```
Map:
ipa: ERROR: 'automountmapautomountmapname' is required
```

This was because Identity Management tries to hide the LDAP implementation and often provides a different value for options and errors than is actually used. It may also use contrived internal names for uniqueness. With this update, Identity Management returns the correct values depending on the context so that a more useful error message is returned. As a result, in the aforementioned scenario, the correct value, ***automountmap***, is now returned.

BZ#714600

The default SSSD configuration did not store passwords if offline. Consequently, when a machine was disconnected from the network, SSSD was unable to authenticate any users. With this update, the ***krb5_store_password_if_offline*** parameter is set to **True** in the **/etc/sssd/sssd.conf** by default. Note that the **--no-krb5-offline-passwords** option of the **ipa-client-install** command may be used if storing passwords for offline use is not desired.

BZ#726722

Passing an empty location to the **automountmap** or **automountkey** command returned the following error:

```
Location:
ipa: ERROR: 'automountlocationcn' is required
```

This was because Identity Management tries to hide the LDAP implementation and often provides a different value for options and errors than is actually used. It may also use contrived internal names

for uniqueness. With this update, Identity Management returns the correct values depending on the context so that a more useful error message is returned. As a result, in the aforementioned scenario, the correct value, ***automountlocation***, is now returned.

BZ#714919

Prior to this update, the **ipa-client-install** command did not configure a hostname in the **/etc/sysconfig/network** file. Consequently, when the **--hostname** value was passed to the client installer, that value was used during enrollment. However, the system hostname did not match the name of the machine. With this update, the **/etc/sysconfig/network** file is updated upon installation and **/bin/hostname** is executed with the hostname of the machine. The name used in the enrollment process now matches the hostname of the machine.

BZ#715112

Renaming users (via **ipa user-mod --setattr**) may have returned a Not Found error. Renaming the actual users was successful, but their user-private groups were not updated. With this update, the **389-ds** plugin has been modified so that the **ipa_modrdn** plugin runs last. This plugin manages renaming of the Kerberos principal name of the user. Renaming a user now also renames the user-private group.

BZ#736684

If an Identity Management client was installed and there was a too large of a time difference between the client and the Identity Management server, a KDC running on the Identity Management server may have refused any Kerberos authentication request from the client. Consequently, the installation process could fail as it could not get a valid Kerberos ticket. With this update, time is always synchronized with the NTP servers configured for the client domain or the Identity Management server itself. If the time synchronization succeeds, the time on the client machine is fixed and Kerberos authentication and the installation itself successfully continue.

BZ#737048

The **ipa-client-install** command always ran **/usr/sbin/authconfig** to add the ***pam_krb5.so*** entry to PAM configuration files in the **/etc/pam.d/** directory. However, this entry was not needed when an Identity Management client is installed with SSSD support, which is the default behavior. As a result, an unnecessary record was added to the PAM configuration. With this update, **/usr/sbin/authconfig** is not run if the Identity Management client is configured with SSSD support.

BZ#717724

The certificate subject base was editable post-install which caused the change to not be propagated to the CA. With this update, the certificate subject base is read-only and the value cannot be modified post installation.

BZ#737581

Prior to this update, a new host could be added to an Identity Management server without proper validation. For example, a host with an invalid hostname or a hostname containing a whitespace character could be created. With this update, proper validation of hostnames for any host has been added, and only hosts with valid hostnames can now be added to an Identity Management server.

BZ#717965

The Identity Management configuration stored a value for *Password Expiration Notification* but did not display it by default (when using the **ipa config-show** command). This update adds *Password Expiration Notification* to the default list of attributes to shown by default when running the **ipa**

config-show command.

BZ#745698

Identity Management installation tools accepted invalid IP addresses in their **--forwarder** or **--ip-address** options. Consequently, installation could eventually fail, for example because of an invalid name server configuration. With this update, all IP addresses passed to the **ipa-server-install**, **ipa-replica-install** and **ipa-dns-install** commands are checked for validity.

BZ#739040

When the **ipa-client-install** command detected that the client hostname was not resolvable, it tried to add a DNS record to the Identity Management server. However, it did not expect that the client could have been using an IPv6 machine, and the installation process failed. This update adds a check to make sure that the process for adding a DNS record to the Identity Management server works for both IPv4 and IPv6, and the Identity Management client installation works as expected.

BZ#739640

When a new service was added via the **Add New Service** Web UI dialog box, the Web UI did not check if the service name field was filled in. When the dialog box was confirmed with the service name field empty, a new service named **undefined** was created. With this update, the service name field is required to be filled in.

BZ#693496

Prior to this update, the **ipa-nis-manage** tool crashed with a python exception when attempting to use an LDAPI connection only. With this update, **ipa-nis-manage** correctly falls back to GSSAPI or a password-based authentication if the LDAPI connection fails.

BZ#723233

An attempt to create a rule with an invalid type returned an error which informed users that only **allow** and **deny** are accepted as types:

```
ipa: ERROR: invalid 'type': must be one of (u'allow', u'deny')
```

However, rules of the type **deny** are not allowed. With this update, the **deny** type was deprecated because SSSD determined that properly enforcing the **deny** type was extremely difficult and dependent on how other libraries present host information.

BZ#743680

The **ipa-server-install** command did not update the system hostname when it was installed with a custom hostname. It passed the hostname to services using their own configurations. However, some services failed to function properly as they did not expect an Identity Management server to use a custom hostname and not a system hostname. With this update, the system hostname is updated to the value passed via **ipa-server-install**'s **--hostname** option. The system hostname is also set in the system network configuration in **/etc/sysconfig/network** so that it is properly set after a system reboot. Refer to Section 2.8, “Authentication” for a known limitation regarding Identity Management server installations with custom hostnames.

BZ#707001

When installing an Identity Management server and using an external CA to sign it, the specified command line options were not properly validated. In such a case, the resulting CSR contained only the string **null**. This update adds better detection of whether the CA 389-ds instance has been

installed to identify the current stage of the installation, thus fixing this issue.

BZ#723778

When deleting an automount location, the command appeared to be successful, but there was no feedback provided on the output. With this update, a summary of all automount commands is shown.

BZ#723781

When adding an automount location, the command appeared to be successful, but there was no feedback provided on the output. With this update, a summary of all automount commands is shown.

BZ#707133

Prior to this update, the **`ipa-nis-manage`** command did not return an exit status of **`0`** when successful. With this update, the underlying source code has been modified to address this issue, and correct exit codes are returned.

BZ#737997

When a new user was added, its login was normalized and lower-cased. However, its principal was not normalized and contained the original login. Consequently, if a new user with an uppercase letter in its login was added, a disconnect between a user login and its principal was created. The Identity Management server then refused to create a password for that user. This update normalizes both the new user long and its principal, thus fixing this issue.

BZ#737994

Certain Identity Management commands require a file to be passed. For example, a cert-request command requires a CSR file. If the command contains a validation rule for the required file, it needs to be executed before it can be processed. However, if the file was passed in the CLI command interactively (and not as a command option), the validation rule was applied to the file path and not the file contents. As a result, a validation rule could fail and the command then returned an error until the file was passed as a command option. With this update, a validation rule is applied to file contents only, and users can pass the required file on the command line both interactively and via a command option.

BZ#726454

Previously, there was no indicator in a host entry that a one-time password was set. This update adds a new output attribute for host entries, **`has_password`**, that is set when the host has a password set. If **`has_password`** is True, a password has been set on the host. However, there is no way to see what that password is once it has been set.

BZ#716287

When a host is enrolled, the user that does the enrollment is stored in the attribute ***`enrolledBy`*** on the host. Prior to this update, an administrator was able to change this value by using the **`ipa host-mod --setattr`**. This action should not be allowed. This update fixes this behavior and write permissions have been removed from the ***`enrolledBy`*** attribute.

BZ#714924

When configuring an Identity Management client to use SSSD, if an error occurred while looking up users, the following error message was displayed:

```
nss_ldap is not able to use DNS discovery
```

This update modifies this error message to be more specific.

BZ#736617

The **ipa-client-install** command did not configure /**usr**/**sbin**/**ntpdate** to use correct NTP servers in the **/etc/ntp/step-tickers**. Additionally, the **ipa-client-install** did not store the state of the **ntpd** service before installation. Consequently, when an Identity Management client is installed, **ntpdate** may have used incorrect servers to synchronize with. When the Identity Management client was uninstalled, the **ntpd** may have been set to an incorrect state. With this update **ipa-client-install** configures **ntpdate** to use the IPA NTP server for synchronization. When an IPA client is uninstalled, both **ntpdate** configuration and **ntpd** status are restored.

BZ#714597

The IPA-generated **/etc/krb5.conf** file contained values which were not present in the standard configuration file (specifically: ***ticket_lifetime***, ***renew_lifetime***, and ***forwardable*** in the **[libdefaults]** section, and the entire **[appdefaults]** section). This update removes these unnecessary values and sections.

BZ#680504

DNS forward and reverse entries are stored discretely. Removing one does not remove the other unless specifically requested. Previously, it was unclear how to remove the required entries. This update adds a new interactive mode (via **ipa dnsrecord-del**) to the command line application which guides the user through the process of removing the required entries.

BZ#725763

Summary data displayed when adding an automount key has been modified to include the map and the key.

BZ#717625

Updating values in the configuration tab in the Identity Management Web UI returned an error. This was because the Web UI was searching for a primary key configuration. With this update, it no longer searches for the key, and the configuration tab works as expected.

BZ#717020

When activating or deactivating a user in the Identity Management Web UI, the user is updated without having to click the **Update** button. With this update, a message box is displayed indicating that the change is going into effect immediately.

BZ#716432

If 389-ds debugging was enabled, superfluous content appeared in the **ipactl** output. With this update, the amount of information displayed in the **ipactl** output has been reduced. The previously reported data is not available in the 389-ds error log only.

BZ#714799

The **ipa-client-install** did not successfully run on a client when a one-time password was set on a host in the Identity Management Web UI. Consequently, clients could not be enrolled using a one-time password if it was set in the Web UI. With this update, the ***krbLastPwdChange*** value is no longer set in the host entry when setting a host one-time password, thus fixing this issue.

BZ#713798

Prior to this update, DNS lookups were not being forwarded if they originated in a subnet that was not managed by Identity Management. With this update, the Identity Management DNS is configured to allow recursion by default, thus fixing this issue.

BZ#713481

When removing a ***runAsGroup*** value from a sudo rule, the command appeared to be successful, but the group information data included in the output was not updated and did not show the proper membership. This update fixes this bug, and data is refreshed before being returned.

BZ#713380

When removing a ***runasuser*** (via **ipa sudorule-remove-runasuser**) and, consequently, defining a group, the *RunAs Group* value was not included in the output. This was because the label for the returned data was mislabeled and was not appearing in the output. With this update, the underlying source code has been modified to address this issue, and adding a group to ***runasuser*** is properly displayed.

BZ#713069

Comma-separated values were not handled properly when the **--externaluser** option was specified for the **sudorule-mod** command. As a result, erroneous values were stored in the entry. With this update, the **--externaluser** option was removed from the **sudorule-mod** command. It is advisable to use the **sudorule-add-user** command instead.

BZ#731804

Upgrading Identity Management from version 2.0.0-23 caused the 389-ds configuration to be modified to not accept requests. With this update, the upgrade process is more robust and always restores the 389-ds configuration. As a result, upgrading Identity Management no longer leaves the system in an inconsistent state.

BZ#731805

Different error types could cause various error messages to appear in the Identity Management Web UI. This update makes all error messages in the Web UI consistent.

BZ#732084

Disabling SELinux (**SELINUX=disabled** in **/etc/selinux/config**) and attempting to restart the **ipa** service caused the **ipa** service to fail to start. This update ignores the value returned by **restorecon**, and the **ipa** service now starts as expected whether SELinux is enabled or disabled.

BZ#712889

A request to set a certificate revocation reason to 7 would cause the request to fail and the certificate was not revoked. Reason 7 is not a valid revocation reason according to RFC 5280. With this update, an error message is returned to the user, informing of the fact that, when used, reason 7 is not a valid revocation reason.

BZ#726028

Previously, renaming an automount key did not work properly because DN of the key was being updated but not the value within the entry. Renaming an automount key now updates the DN and the stored key value, thus fixing this issue.

BZ#711786

When setting **runAsGroup** in a sudo role as a user, the name of that user is returned as the name of

a group that may also be used as the **runAsGroup**. As a result, the sudo rule was erroneous and referred to a non-existent group. This was because the search filter for determining the CN value was too generic. This update adds a test which assures user names no longer appear as **runAsGroup** values.

BZ#711761

Prior to this update, removing a sudo rule option failed on the server because the code which handled sudo rule option removal was not robust enough and if the input did not exactly match the stored value, it failed. With this update, removing sudo rule options works as expected.

BZ#711671, BZ#711667

Previously, comma-separated values were not handled properly when using **sudorule-mod**'s **--runasexternaluser** or **--runasexternalgroup** options. With this update, the aforementioned options have been deprecated. It is advisable to use the **sudorule-add-runasuser** or **sudorule-runasgroup** commands instead.

BZ#710601, BZ#710598, BZ#710592

Prior to this update, leading and trailing spaces were allowed in some parameter values. This update adds a validator that disallows the use of leading and trailing spaces.

BZ#710530

Passing an empty password when prompted to by the **ipa-nis-manage** command did not display an error and did not exit the command. With this update, passing an empty password causes an error to appear (**No password supplied**), and the command is exited with the status code **1**.

BZ#710494

The **ipa-nis-manage** command has an option, **-y**, to specify the Directory Manager password in a file. This option caused the command to crash if the file did not exist. An exception handler around the password reader has been added, and a proper error message is displayed when the supplied password file is non-existent or is not readable.

BZ#710253

When adding a ***runasuser*** (via **ipa sudorule-add-runasuser**) and, consequently, defining a group, the *RunAs Group* value was not included in the output. This was because the label for the returned data was mislabeled and was not appearing in the output. With this update, the underlying source code has been modified to address this issue, and adding a group to ***runasuser*** is properly displayed.

BZ#738693

A user with a valid Kerberos ticket can change an IPA password with the **ipa passwd** command. Prior to this update, the command did not require entering the old password. Consequently, anyone with access to that user's shell could change his Identity Management password without knowing the old password. With this update, the old password is always required in order to change a user's password. The only exception is the administrator user.

BZ#710245

A removed sudorule option appeared in the output when that option was removed. With this update, option values are refreshed before being returned, and the output of the delete command is consistent with the actual data.

BZ#710240

Adding a duplicate sudorule option did not generate any errors messages. With this update, rather than ignoring duplicate values, an error is returned when a duplicate sudorule option is added.

BZ#739195

When attempting to unprovision a host keytab in the Identity Management Web UI Unprovisioning Host dialog, there was no option to cancel the process. This update adds the **`Cancel`** button to the Unprovisioning Host dialog.

BZ#709665, BZ#709645

When removing external hosts from a sudorule, the output shown after the command completed contained the hosts that were removed. With this update, external host information is refreshed before it is returned to the client.

BZ#707312

Previously, new DNS zones were not available until the **`bind`** service was restarted. With this update, an updated bind-dyndb-ldap package added a zone refresh option that Identity Management uses to refresh the zone list in DNS. The default setting is 30 seconds. As a result, new DNS zones are not immediately available, but the **`bind`** service does not have to be restarted anymore.

BZ#740320

When a new group was being created via the Identity Management Web UI, unchecking the Posix check box was not taken into account and a posix group was created every time. With this update, the underlying source code has been modified to address this issue, and creating non-posix groups works as expected.

BZ#707229

The **`--no-host-dns`** option of the **`ipa-server-install`** command still checked that the forward and reverse DNS entries existed and matched. Installation of an Identity Management server using a host name that could not be resolved would then fail. This update removes any DNS validation when the **`--no-host-dns`** option is used.

BZ#705804

The subject name of a CA agent certificate used by Identity Management was not very specific. This update changes the subject name from **`RA Subsystem`** to **`IPA RA`**.

BZ#702685

If a remote LDAP server that was being used while migrating to Identity Management contained an LDAP search reference, the migration failed. With this update, the migration process logs any search references and skips them, assuring a successful migration.

BZ#740885

For an HBAC rule, you can choose to add a host in the **`Accessing`** section of the Identity Management Web UI. Clicking on **`Enroll`** without selecting a host did not return an error indicating that a host was not selected. With this update, the **`Enroll`** button is disabled until a host is chosen.

BZ#740891

For an HBAC rule, you can choose to delete a host in the **Accessing** section of the Identity Management Web UI. Clicking on **Enroll** without selecting a host did not return an error indicating that a host was not selected. With this update, the **Enroll** button is disabled until a host is chosen.

BZ#741050

The **ipa-client-install** command always checked the specified server whether it was a valid Identity Management server. However, if the Identity Management server was configured to restrict access for anonymous binds (via the **nsslapd-allow-anonymous-access** option), the check failed and the installation processes returned an error and ended. With this update, when the **ipa-client-install** command detects that the chosen server does not allow anonymous binds, it skips server verification, reports a warning, and lets the user join the Identity Management server.

BZ#701325

The X509v3 certificate shown in a host or service record in the Identity Management Web UI was not properly formatted. This update converts the certificate from the base64 format to the PEM format.

BZ#698219

The Apache service communicates with 389-ds early on during the start-up (to attempt to retrieve the LDAP schema). Previously, if that communication failed, the Apache service would have to be restarted. This race condition could cause a restarted Identity Management server become unavailable. With this update, the communication between Apache and 389-ds is retried when it fails, thus fixing this issue.

BZ#697878

The Identity Management server installation could fail with an error informing of the fact that the LDAP server could not be reached. This was because the installation process did not wait for the 389-ds server to fully start after a restart. With this update, the installation process waits for the 389-ds server to be fully started.

BZ#742875

When an Identity Management server was installed, it did not properly check the system's static lookup table (**/etc/hosts**) for records which could interfere with its IP address or hostname, and cause forward or reverse DNS queries to be resolved to different values than expected. The installation process now always checks for any conflicting records in the **/etc/hosts** file.

BZ#696282

A certificate subject base with an incorrect format provided by the user could cause an installation process to fail in the CA step with a non-descriptive error. With this update, the subject base of a certificate is validated, and the installation no longer fails.

BZ#696268

Providing an IP address during the Identity Management server installation via the **--ip-address** option caused the installed server to not function properly. With this update, it is verified whether the provided IP address is a configured interface on the system. Providing an IP address that is not associated with a local network interface will return an error message.

BZ#743788

The IPA Web UI was missing a title on several pages. This update adds the missing titles.

BZ#693771

Including non-ASCII characters in the ***zonemgr*** email address could cause an installation to fail with an unclear message. This update adds a validator which requires the ***zonemgr*** to contain ASCII characters only.

BZ#681978

Uninstalling an Identity Management client on a machine which has the Identity Management server installed on it as well caused the server to break. The client uninstaller now detects the installation state of an installed server. An attempt to uninstall a client from a machine which also contains the server will result in an error message. The client can be uninstalled when the server is uninstalled.

BZ#744024

Prior to this update, the **`ipa-client-install`** command did not return an exit status of **`0`** when successful. With this update, the underlying source code has been modified to address this issue, and correct exit codes are returned.

BZ#744074

Prior to this update, the Identity Management Web UI allowed a user to delete a global Password Policy. If a global Password Policy is deleted, any attempt to add a user with a Kerberos password fails. Additionally, neither the CLI nor the Web UI version of Identity Management could be used to add this policy back. With this update, deleting the global Password Policy is denied.

BZ#692955

Attempting to set the manager value of a user resulted in the following error message:

```
value #0 invalid per syntax: Invalid syntax.
```

This was because the value required a full LDAP DN syntax. With this update, when storing or retrieving the manager value, the value is automatically translated between a login name and a DN. Setting the manager value now requires a login name only.

BZ#744422

During the installation of a Identity Management server, the **`ipa-server-install`** called **kdb5_ldap_util** to populate the directory with realm information. In the process of doing so, it passes the Kerberos master database password and the Kerberos directory password as parameters. As a result, a user could list all running processes during the IPA server installation and discover the aforementioned passwords. With this update, **kdb5_ldap_util**'s interactive mode is used to pass the passwords instead of passing them via CLI parameters.

BZ#692950

When setting up DNS during an interactive installation, a reverse zone was always created regardless of the **`--no-reverse`** option. This update fixes this behavior, and a reverse zone is not created unless specified.

BZ#745392

When the **`ipa-client-install`** command attempted to auto-discover the Identity Management server in its domain, it did not use any timeout when a server was found and was being checked. If the found server was unresponsive during the auto-discovery, the **`ipa-client-install`** command got stuck and did not continue. This update adds a 30 second timeout to the **`ipa-client-install`** auto-discovery server check.

BZ#692144

Using the **--no-sssd** option of the **ipa-client-install** command did not properly back up and restore the existing **/etc/sssd/sssd.conf** file. With this update, the underlying source code has been modified to address this issue, and the **--no-sssd** option works as expected.

BZ#690473

Using the **--hostname** option to set a value outside an Identity Management-managed DNS domain did not return an error and did not add the host to DNS. The DNS updating utility, **nsupdate**, was modified to properly return an error when an update fails.

BZ#690185

Uninstalling an Identity Management client did not restore certain files when that client was previously installed with the **--force** option. This was because the **--force** option was able to re-install over an already installed system, causing the original saved files to be lost. This behavior is no longer permitted; the client must be first uninstalled and only then it can be re-installed.

BZ#689810

Adding a duplicate user resulted in a generic error message which was not specific enough to discover the reason of the error. With this update, the object type and the primary key are returned in the error message, making the error message more understandable.

BZ#689023

When adding a new password policy, the Identity Management Web UI did not prompt for a required field, **priority**. This update requires the **priority** field to be filled in.

BZ#688925

The process of setting up an Identity Management replica became unresponsive if the master could not be reached. This update adds a new utility, **ipa-replica-conncheck**, which verifies that the replica and the master can communicate in both directions.

BZ#688266

If the domain did not match the realm, enrolling a client could fail with the following error:

```
Cannot resolve network address for KDC
```

This was because a temporary **/etc/krb5.conf** file was used during enrollment to contact the Identity Management KDC. The process was always relying on DNS auto-discovery to find the correct KDC and not the values provided by the end-user. With this update, enrollment works even if the domain does not match the realm.

BZ#683641

If a one-time password was set on a host, an administrator was unable to enroll it and the following error message would be returned:

```
No permission to join this host to the IPA domain.
```

A delegated administrator did not have permissions to write the Kerberos principal name. This update adds permissions for the delegated administrator to be able to add a one-time password, but not change or remove an existing one.

BZ#681979

The `--on-master` lacked proper documentation. This update makes the option invisible and removes it from documentation entirely.

BZ#747443

Realm-Domain mapping was not specified in a client's Kerberos configuration when the client was outside of an Identity Management domain. In such a case, Certmonger would fail to issue a host certificate. Realm-Domain mapping is now properly configured when the client is outside of the Identity Management domain.

BZ#748754

Arguments for the Kerberos KDC, contained in the `/etc/sysconfig/krb5kdc` file, were not formatted properly on multi-CPU systems. As a consequence, the KDC could not use the intended number of CPUs and reported an error when it was (re)started. With this update, the aforementioned arguments are now properly formatted, fixing this issue.

BZ#749352

Prior to this update, the `ypcat` command's netgroup output did not show users in netgroup triples. Consequently, NIS-based authorization did not work as expected, and access was denied when it should have been allowed. This was caused by a syntax error in the triple rule. This update fixes this error, and users are now properly included in the netgroup triples.

BZ#736170

The ipa package has been upgraded to upstream version 2.1.3 which provides a number of bug fixes and enhancements over the previous version.

Users are advised to upgrade to these updated ipa packages, which resolve these issues.

4.95. IPA-PKI-THEME

4.95.1. RHBA-2011:1754 — ipa-pki-theme bug fix update

Updated ipa-pki-theme packages which fix this bug are now available for Red Hat Enterprise Linux 6.

The ipa-pki-theme packages provide Red Hat Identity Management theme components for PKI packages.

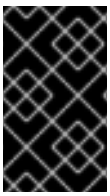
Certificate System (CS) manages enterprise Public Key Infrastructure (PKI) deployments and requires a theme for the specific type of PKI deployment with which it is used. This package makes a Red Hat Identity Management theme available for CS, and therefore makes it possible for users of Red Hat Enterprise Linux 6 to use CS as a part of Red Hat Identity Management deployments.

Bug Fix

BZ#712931

IPA (Identity, Policy and Audit) is an identity and access management system. Prior to this update, Certificate System (CS), which is implemented in pki-core, required multiple ports to be open in a firewall for IPA to work. The number of open ports required has been reduced, and support for a proxy using Apache JServ Protocol (AJP) ports has been added, by enhancements made in pki-core. With

this update, ipa-pki-theme has been changed to make use of the updates to CS, including adding the proxy-ipa.conf configuration file, and fixing broken links in certain user interface files. As a result, it is now possible for ipa-pki-theme to support running CS behind a proxy Apache server.



IMPORTANT

This theme is mutually exclusive with the PKI themes for other types of PKI deployments, such as dogtag-pki-theme for Dogtag Certificate System deployments and redhat-pki-theme for Red Hat Certificate System deployments. (BZ#643543)

All users of ipa-pki-theme are advised to upgrade to these updated packages, which fixes this bug.

4.96. IPMITOOL

4.96.1. RHSA-2011:1814 — Moderate: ipmitool security update

An updated ipmitool package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The ipmitool package contains a command line utility for interfacing with devices that support the Intelligent Platform Management Interface (IPMI) specification. IPMI is an open standard for machine health, inventory, and remote power control.

Security Fix

CVE-2011-4339

It was discovered that the IPMI event daemon (ipmievd) created its process ID (PID) file with world-writable permissions. A local user could use this flaw to make the ipmievd init script kill an arbitrary process when the ipmievd daemon is stopped or restarted.

All users of ipmitool are advised to upgrade to this updated package, which contains a backported patch to correct this issue. After installing this update, the IPMI event daemon (ipmievd) will be restarted automatically.

4.96.2. RHBA-2011:1603 — ipmitool bug fix update

An updated ipmitool package that fixes multiple bugs is now available for Red Hat Enterprise Linux 6.

The ipmitool package contains a command line utility for interfacing with devices that support the Intelligent Platform Management Interface (IPMI) specification. IPMI is an open standard for machine health, inventory, and remote power control.

Bug Fixes

BZ#675975

Prior to this update, ipmitool's Serial Over LAN (SOL) module erroneously calculated the number of octets processed by the Baseboard Management Controller and could have resent already

acknowledged chunks of serial communication, which could have corrupted the serial line with additional characters. Under certain circumstances, this could have also brought ipmitool into an endless loop or unexpected termination. With this update, ipmitool now correctly calculates the number of octets processed by the BMC and does not resend unwanted characters over the serial line.

BZ#727314

This update improves integration of the Linux Multiple Device (MD) driver with ipmitool to indicate the SCSI enclosure services (SES) status and drive activities for the PCIe SSD based solutions.

BZ#726390

This update adds the "channel setkg" subcommand to the "ipmitool" command, which allows for KG key configuration.

BZ#726390

This update adds the "-Y" option, which allows reading of the KG key from the terminal.

BZ#731977

A serial console connected to over the LAN and activated with the command "ipmitool sol activate" contained a memory leak, which could have consumed all available memory resources over time. This update fixes the problem.

BZ#731718

Invoking "ipmitool delloem powermonitor" did not properly convert values received over the network to integer numbers on big-endian systems (PowerPC, IBM System z). As a result, mostly random values were displayed when reporting power consumption. This update fixes the integer conversions in the "powermonitor" command so that the power consumption is now reported correctly on PowerPC and IBM System z architectures.

All users of ipmitool are advised to upgrade to this updated package, which fixes these bugs.

4.96.3. RHBA-2013:1164 — ipmitool bug fix update

Updated ipmitool packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The ipmitool package contains a command-line utility for interfacing with devices that support the Intelligent Platform Management Interface (IPMI) specification. IPMI is an open standard for machine health, inventory, and remote power control.

Bug Fix

BZ#990960

In cases of congested networks or slow-responding BMCs (Baseboard Management Controller), the reply operation timeout triggered the protocol command retry action. Consequently, the ipmitool utility could incorrectly process a LAN session protocol command with the reply from a previous protocol command. This update fixes handling of expected replies for each command alone and cleans up expected replies between commands. Now, the retried reply of the first command is correctly ignored while the later command, which is currently pending, is properly processed in the described scenario.

Users of ipmitool are advised to upgrade to these updated packages, which fix this bug. After installing this update, the IPMI event daemon (ipmievd) will be restarted automatically.

4.97. IPROUTE

4.97.1. RHBA-2011:1690 — iproute bug fix update

An updated iproute package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The iproute package contains networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux kernel.

Bug Fixes

BZ#692867

Prior to this update, the "ip" utility lacked the "mode" parameter support for macvtap devices. As a consequence affected users could not create macvtap devices in "bridge" or "private" modes. With this update the "ip" utility now fully supports macvtap devices along with the "mode" parameter and its options, "bridge", "private", and "vepa" (default). As a result users can now utilize macvtap functionality via the iproute package.

BZ#693878

Prior to this update, the "ip" tool lacked the "passthru" mode parameter support for macvtap and macvlan devices. Consequently users could not create macvtap and macvlan devices in "passthru" mode. The "ip" tool now fully supports macvtap and macvlan devices along with the "mode" parameter and its options, "bridge", "private", "passthru", and "vepa" (default). As a result users can now utilize "passthru" mode as part of macvtap and macvlan functionality via the iproute package.

BZ#709652

Prior to this update, the "tc" utility ignored GRED (Generalized RED) queue options. Consequently "tc" users could not configure certain GRED queue related parameters. With this update the "tc" utility no longer accidentally overwrites the user specified options. As a result "tc" users can now reliably define all GRED parameters.

All users of iproute are advised to upgrade to this updated package, which fixes these bugs.

4.98. IPRUTILS

4.98.1. RHEA-2011:1546 — iprutils bug fix and enhancement update

An updated iprutils package that fixes various bugs and provides one enhancement is now available for Red Hat Enterprise Linux 6.

The iprutils package provides utilities to manage and configure SCSI devices that are supported by the IBM Power RAID SCSI storage device driver.

The iprutils package has been upgraded to upstream version 2.3.4, which provides support for the Serial Attached SCSI (SAS) vRAID functions. (BZ#693816)

Bug Fixes

BZ#694756

Due to a NULL pointer dereference, the iprconfig utility terminated unexpectedly with a segmentation fault when attempting to display hardware status. A patch has been applied to address this issue and hardware status is now displayed correctly.

BZ#703255

Previously, iprutils did not work correctly when performing RAID migration and asymmetric access functions on new adapters. With this update, array migration functionality is fixed. Now, iprutils can correctly perform the raid migration and asymmetric access functions.

BZ#741835

The find_multipath_vset routine used the ARRAY_SIZE() macro to calculate the length of the serial number. Previously, the length was calculated incorrectly, which could have led to false positives when looking for the corresponding vset. As a consequence, attempting to delete arrays failed: the target and the second array were set to be read/write protected, writing to both arrays was not possible, and the system had to be rebooted. To fix the problem, the IPR_SERIAL_NUM_LEN macro is now used instead of ARRAY_SIZE.

BZ#741835

With the maximum number of devices attached to one of the new Silicon Integrated Systems (SiS) 64-bit adapters, the configuration data could have grown over the buffer size. With this update, the buffer size has been increased, which fixes the problem and ensures room for any possible future growth.

All users of iprutils are advised to upgrade to this updated package, which fixes these bugs and provides this enhancement.

4.99. IPTABLES

4.99.1. RHBA-2012:0335 — iptables bug fix update

Updated iptables packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The iptables utility controls the network packet filtering code in the Linux kernel.

Bug Fix

BZ#786874

The option parser of the iptables utility did not correctly handle the "-m mark" and "-m conmark" options in the same rule. Therefore, the iptables command failed when issued with both options. This update modifies behavior of the option parser so that iptables now works as expected with the "-m mark" and "-m conmark" options specified.

All users of iptables are advised to upgrade to these updated packages, which fix this bug.

4.100. IRQBALANCE

4.100.1. RHBA-2012:0552 — irqbalance bug fix update

Updated irqbalance packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The irqbalance package provides a daemon that evenly distributes interrupt request (IRQ) load across multiple CPUs for enhanced performance.

Bug Fix

BZ#817873

The irqbalance daemon assigns each interrupt source in the system to a "class", which represents the type of the device (for example Networking, Storage or Media). Previously, irqbalance used the IRQ handler names from the /proc/interrupts file to decide the source class, which caused irqbalance to not recognize network interrupts correctly. As a consequence, systems using biosdevname NIC naming did not have their hardware interrupts distributed and pinned as expected. With this update, the device classification mechanism has been improved, and so ensures a better interrupts distribution.

All users of irqbalance are advised to upgrade to these updated packages, which fix this bug.

4.101. ISCSI-INITIATOR-UTILS

4.101.1. RHBA-2011:1722 — iscsi-initiator-utils bug fix and enhancement update

An updated iscsi-initiator-utils package that fixes one bug and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The iscsi package provides the server daemon for the Internet Small Computer System Interface (iSCSI) protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

Bug Fix

BZ#715434

The iscsiadm utility displayed the discovery2 mode in the help output but did not accept the mode as a valid one. This entry has been replaced with the valid discoverydb mode entry as displayed in the ISCSIADM(8) manual page.

Enhancements

BZ#602959

The brcm_iscsiuio daemon did not rotate its log file, /var/log/brcm-iscsi.log. As a consequence, the log file may have filled up the available disk space. The brcm_iscsiuio daemon now supports log rotation, which fixes the problem.

BZ#696808

The brcm_iscsiuio daemon has been updated to provide enhanced support for IPv6 (Internet Protocol version 6), VLAN (Virtual Local Area Network), and Broadcom iSCSI Offload Engine Technology. The daemon has been renamed to iscsiuio with this update.

BZ#749051

The bnx2i driver can now be used for install or boot. To install or boot to targets using this driver, turn on the HBA (Host Bus Adapter) mode in the card's BIOS boot setup screen.

In addition, the iSCSI tools can now set up networking and manage sessions for QLogic iSCSI adapters that use the qla4xxx driver. For more information, see section 5.1.2 of the README file which is located in the /usr/share/doc/iscsi-initiator-utils-6.2.0.872 directory.

Users are advised to upgrade to this updated iscsi-initiator-utils package, which fixes this bug and adds these enhancements.

4.102. ISDN4K-UTILS

4.102.1. RHBA-2011:1169 — isdn4k-utils bug fix update

Updated isdn4k-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The isdn4k-utils package contains a collection of utilities needed for configuring an ISDN subsystem.

Bug Fixes

BZ#618653

Prior to this update, the isdn and capi init scripts were not LSB compatible. Due to this problem, the isdn and capi init scripts exited with incorrect or invalid exit statuses. This update modifies the init scripts so that they are LSB compatible. Now the init scripts exit with the correct exit status. (BZ#618549)

All users of isdn4k-utils are advised to upgrade to these updated packages, which fix this bug.

4.103. IWL1000-FIRMWARE

4.103.1. RHBA-2011:1558 — iwl1000-firmware bug fix and enhancement update

An updated iwl1000-firmware package that fixes various bugs and adds several enhancements is now available for Red Hat Enterprise Linux 6.

The iwl1000-firmware package provides the firmware required by the iwglan driver for Linux to support Intel Wireless WiFi Link 1000 series adapters.

The iwl1000-firmware package has been upgraded to upstream version 39.31.5.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#694245)

All users of the iwlagn driver are advised to upgrade to this updated iwl1000-firmware package, which resolves these issues and adds these enhancements.

4.104. IWL6000G2A-FIRMWARE

4.104.1. RHEA-2011:1681 — iwl6000g2a-firmware enhancement update

An updated iwl6000g2a-firmware package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The iwl6000g2a-firmware package provides the firmware required by the iwlagn driver for Linux to support Intel Wireless WiFi Link 6005 series adapters.

The iwl6000g2a-firmware package has been upgraded to upstream version 17.168.5.3, which provides an enhancement over the previous version. (BZ#729438)

All users of the iwlagn driver are advised to upgrade to this updated iwl6000g2a-firmware package, which adds this enhancement.

4.105. JASPER

4.105.1. RHSA-2011:1807 — Important: jasper security update

Updated jasper packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

JasPer is an implementation of Part 1 of the JPEG 2000 image compression standard.

Security Fix

CVE-2011-4516, **CVE-2011-4517**

Two heap-based buffer overflow flaws were found in the way JasPer decoded JPEG 2000 compressed image files. An attacker could create a malicious JPEG 2000 compressed image file that, when opened, would cause applications that use JasPer (such as Nautilus) to crash or, potentially, execute arbitrary code.

Red Hat would like to thank Jonathan Foote of the CERT Coordination Center for reporting these issues.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. All applications using the JasPer libraries (such as Nautilus) must be restarted for the update to take effect.

4.106. JAVA-1.5.0-IBM

4.106.1. RHSA-2012:0508 — Critical: java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

Security Fixes

CVE-2011-3389, **CVE-2011-3557**, **CVE-2011-3560**, **CVE-2011-3563**, **CVE-2012-0498**, **CVE-2012-0499**, **CVE-2012-0501**, **CVE-2012-0502**, **CVE-2012-0503**, **CVE-2012-0505**, **CVE-2012-0506**, **CVE-2012-0507**

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.5.0 SR13-FP1 Java release. All running instances of IBM Java must be restarted for this update to take effect.

4.107. JAVA-1.6.0-IBM

4.107.1. RHSA-2012:0514 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM Java SE version 6 release includes the IBM Java 6 Runtime Environment and the IBM Java 6 Software Development Kit.

Security Fixes

CVE-2011-3563, **CVE-2011-5035**, **CVE-2012-0497**, **CVE-2012-0498**, **CVE-2012-0499**, **CVE-2012-0500**, **CVE-2012-0501**, **CVE-2012-0502**, **CVE-2012-0503**, **CVE-2012-0505**, **CVE-2012-0506**, **CVE-2012-0507**

This update fixes several vulnerabilities in the IBM Java 6 Runtime Environment and the IBM Java 6 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM Java 6 SR10-FP1 release. All running instances of IBM Java must be restarted for the update to take effect.

4.107.2. RHSA-2012:0034 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM Java SE version 6 release includes the IBM Java 6 Runtime Environment and the IBM Java 6 Software Development Kit.

Security Fixes

CVE-2011-3389, **CVE-2011-3516**, **CVE-2011-3521**, **CVE-2011-3544**, **CVE-2011-3545**, **CVE-2011-3546**, **CVE-2011-3547**, **CVE-2011-3548**, **CVE-2011-3549**, **CVE-2011-3550**, **CVE-2011-3551**, **CVE-2011-3552**, **CVE-2011-3553**, **CVE-2011-3554**, **CVE-2011-3556**, **CVE-2011-3557**, **CVE-2011-3560**, **CVE-2011-3561**

This update fixes several vulnerabilities in the IBM Java 6 Runtime Environment and the IBM Java 6 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM Java 6 SR10 release. All running instances of IBM Java must be restarted for the update to take effect.

4.108. JAVA-1.6.0-OPENJDK

4.108.1. RHSA-2012:0135 — Critical: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2012-0497

It was discovered that Java2D did not properly check graphics rendering objects before passing them to the native renderer. Malicious input, or an untrusted Java application or applet could use this flaw to crash the Java Virtual Machine (JVM), or bypass Java sandbox restrictions.

CVE-2012-0505

It was discovered that the exception thrown on deserialization failure did not always contain a proper identification of the cause of the failure. An untrusted Java application or applet could use this flaw to bypass Java sandbox restrictions.

CVE-2011-3571

The AtomicReferenceArray class implementation did not properly check if the array was of the expected Object[] type. A malicious Java application or applet could use this flaw to bypass Java sandbox restrictions.

CVE-2012-0503

It was discovered that the use of TimeZone.setDefault() was not restricted by the SecurityManager, allowing an untrusted Java application or applet to set a new default time zone, and hence bypass Java sandbox restrictions.

CVE-2011-5035

The HttpServer class did not limit the number of headers read from HTTP requests. A remote attacker could use this flaw to make an application using HttpServer use an excessive amount of CPU time via a specially-crafted request. This update introduces a header count limit controlled using the sun.net.httpserver.maxReqHeaders property. The default value is 200.

CVE-2011-3563

The Java Sound component did not properly check buffer boundaries. Malicious input, or an untrusted Java application or applet could use this flaw to cause the Java Virtual Machine (JVM) to crash or disclose a portion of its memory.

CVE-2012-0502

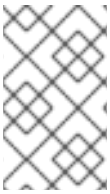
A flaw was found in the AWT KeyboardFocusManager that could allow an untrusted Java application or applet to acquire keyboard focus and possibly steal sensitive information.

CVE-2012-0506

It was discovered that the CORBA (Common Object Request Broker Architecture) implementation in Java did not properly protect repository identifiers on certain CORBA objects. This could have been used to modify immutable object data.

CVE-2012-0501

An off-by-one flaw, causing a stack overflow, was found in the unpacker for ZIP files. A specially-crafted ZIP archive could cause the Java Virtual Machine (JVM) to crash when opened.



NOTE

If the web browser plug-in provided by the icedtea-web package was installed, the issues exposed via Java applets could have been exploited without user interaction if a user visited a malicious website.

This erratum also upgrades the OpenJDK package to IcedTea6 1.10.6. Refer to the NEWS file for more information:

http://icedtea.classpath.org/hg/release/icedtea6-1.10/file/icedtea6-1.10.6/NEWS

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.108.2. RHSA-2012:0729 — Critical: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2012-1711, **CVE-2012-1719**

Multiple flaws were discovered in the CORBA (Common Object Request Broker Architecture) implementation in Java. A malicious Java application or applet could use these flaws to bypass Java sandbox restrictions or modify immutable object data.

CVE-2012-1716

It was discovered that the SynthLookAndFeel class from Swing did not properly prevent access to certain UI elements from outside the current application context. A malicious Java application or applet could use this flaw to crash the Java Virtual Machine, or bypass Java sandbox restrictions.

CVE-2012-1713

Multiple flaws were discovered in the font manager's layout lookup implementation. A specially-crafted font file could cause the Java Virtual Machine to crash or, possibly, execute arbitrary code with the privileges of the user running the virtual machine.

CVE-2012-1723, **CVE-2012-1725**

Multiple flaws were found in the way the Java HotSpot Virtual Machine verified the bytecode of the class file to be executed. A specially-crafted Java application or applet could use these flaws to crash the Java Virtual Machine, or bypass Java sandbox restrictions.

CVE-2012-1724

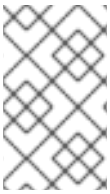
It was discovered that the Java XML parser did not properly handle certain XML documents. An attacker able to make a Java application parse a specially-crafted XML file could use this flaw to make the XML parser enter an infinite loop.

CVE-2012-1718

It was discovered that the Java security classes did not properly handle Certificate Revocation Lists (CRL). CRL containing entries with duplicate certificate serial numbers could have been ignored.

CVE-2012-1717

It was discovered that various classes of the Java Runtime library could create temporary files with insecure permissions. A local attacker could use this flaw to gain access to the content of such temporary files.



NOTE

If the web browser plug-in provided by the icedtea-web package was installed, the issues exposed via Java applets could have been exploited without user interaction if a user visited a malicious website.

This erratum also upgrades the OpenJDK package to IcedTea6 1.11.3. Refer to the NEWS file for further information:

http://icedtea.classpath.org/hg/release/icedtea6-1.11/file/icedtea6-1.11.3/NEWS

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.108.3. RHBA-2011:1623 — java-1.6.0-openjdk enhancement update

An updated java-1.6.0-openjdk package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

This updated java-1.6.0-openjdk package includes fixes for the following bugs:

BZ#722310

The java-1.6.0-openjdk package has been upgraded to the upstream version 1.10.4, which provides a number of bug fixes and enhancements over the previous version.

BZ#708201

Installing of OpenJDK or execution of a Java program, which was using other than terminal fonts, could have terminated unexpectedly with the following error:

```
Exception in thread "main"
java.lang.Error: Probable fatal error:No fonts found.
```

This happened because the fontconfig library was not installed and the font enumeration failed. With this update, OpenJDK depends on fontconfig and the problem no longer occurs.

All users of java-1.6.0-openjdk are advised to upgrade to this updated package, which fixed these bugs.

4.108.4. RHBA-2011:1847 — java-1.6.0-openjdk bug fix update

Updated java-1.6.0-openjdk packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The java-1.6.0-openjdk package provides the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

The java-1.6.0-openjdk package has been upgraded to upstream version 1.2.3, which provides a number of bug fixes and enhancements over the previous version. In addition, HugePage support is now provided and can be activated with the -XX:+UseLargePages flag. (BZ#123456)

Bug Fix

BZ#751730

Prior to this update, security restrictions caused the RMI registry to stop working correctly. As a consequence, a remote RMI client could execute code on the RMI server with unrestricted privileges.This update adjusts the RMI registry so that it now works as expected.

Enhancements

BZ#567404

This update adds support for the Rhino JavaScript interpreter to the java-1.6.0-openjdk package.

BZ#727598

This update upgrades IcedTea6 to upstream version 1.10.

All users of java-1.6.0-openjdk are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.109. JAVA-1.6.0-SUN

4.109.1. RHSA-2012:0734 — Critical: java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

Security Fixes

CVE-2012-0551, **CVE-2012-1711**, **CVE-2012-1713**, **CVE-2012-1716**, **CVE-2012-1717**, **CVE-2012-1718**, **CVE-2012-1719**, **CVE-2012-1721**, **CVE-2012-1722**, **CVE-2012-1723**, **CVE-2012-1724**, **CVE-2012-1725**

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide JDK and JRE 6 Update 33 and resolve these issues. All running instances of Sun Java must be restarted for the update to take effect.

4.109.2. RHSA-2012:0139 — Critical: java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

Security Fixes

CVE-2011-3563, **CVE-2011-3571**, **CVE-2011-5035**, **CVE-2012-0498**, **CVE-2012-0499**, **CVE-2012-0500**, **CVE-2012-0501**, **CVE-2012-0502**, **CVE-2012-0503**, **CVE-2012-0505**, **CVE-2012-0506**

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch page:

- http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html
- http://www.oracle.com/technetwork/java/javase/6u31-relnotes-1482342.html

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide JDK and JRE 6 Update 31 and resolve these issues. All running instances of Sun Java must be restarted for the update to take effect.

4.110. JSS

4.110.1. RHBA-2011:1675 — jss bug fix update

An updated jss package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

JSS is a Java binding to Network Security Services (NSS), which provides SSL/TLS network protocols and other security services in the Public Key Infrastructure (PKI) suite. JSS is primarily utilized by the Certificate Server.

Bug Fixes

BZ#660436

The java.net.SocketException was accompanied by a misleading error message because the exception definition was using a variable pointed to a wrong address. With this update, the underlying code has been modified and the exception now uses the correct error message.

BZ#705947

On Luna SA HSM in FIPS mode, Red Hat Certificate System failed to generate a certificate and threw an exception if ECC (Elliptic Curve Cryptography) algorithms was set to higher than SHA1withEC. This occurred because in FIPS mode, the SSL protocol requires ECDH (Elliptic Curve Diffie Hellman), which is not supported by Luna SA. With this update, the ECDH support has been provided by JSS/NSS, and certificates are created and used with SSL correctly.

BZ#733551

In FIPS mode, DRM (Data Recovery Manager) failed to recover keys because it failed to import the respective key. With this update, the key is generated on recovery and the recovery succeeds.

All users of jss are advised to upgrade to this updated package, which fixes these bugs.

4.111. JWHOIS

4.111.1. RHBA-2011:0921 — jwhois bug fix and enhancement update

An updated jwhois package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The jwhois package provides a whois client, which is used to obtain information about domain names and IP addresses from whois servers.

Bug Fix

BZ#682832

Previously, when querying a domain with the name length near the allowed limit of 63 characters, and emitting command options to a whois server, the "whois" command failed because both the domain name and command options were given to a function responsible for translating Internationalized Domain Names (IDN) to ASCII. The length of such command was greater than the allowed limit. This update fixes this bug so that only the domain name is now translated after executing the command.

Enhancement

BZ#664449

Previously, jwhois did not contain the whois server details for the dotEmarat extension. As a result, whois queries for these extensions were incorrectly directed to whois.internic.net. With this update, the configuration file correctly directs queries for the dotEmarat domains to whois.aeda.net.ae.

All users of whois clients are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.112. KABI-WHITELISTS

4.112.1. RHEA-2011:1747 — kabi-whitelists enhancement update

An updated kabi-whitelists package that adds various enhancements is now available for Red Hat Enterprise Linux 6.

The kabi-whitelists package contains reference files documenting interfaces provided by the Red Hat Enterprise Linux 6 kernel that are considered to be stable by Red Hat kernel engineering, and safe for longer term use by third party loadable device drivers, as well as for other purposes.

Enhancements

BZ#680469

The "pci_reset_function" symbol has been added to the Red Hat Enterprise Linux 6.2 kernel application binary interface (ABI) whitelists.

BZ#690479

The "aio_complete" and "aio_put_req" symbols have been added to the kernel ABI whitelists.

BZ#700406

The "__blk_end_request", "bdget_disk", "blk_limits_io_min", "blk_limits_io_opt", "blk_plug_device", "blk_queue_bounce", "blk_queue_max_discard_sectors", "blk_remove_plug", "blk_requeue_request", "jiffies_to_usecs", "prepare_to_wait_exclusive", "ipv6_ext_hdr", "lro_receive_frags", and "lro_vlan_hwaccel_receive_frags" symbols have been added to the kernel ABI whitelists.

BZ#700432

The "ipv6_ext_hdr", "lro_receive_frags", and "lro_vlan_hwaccel_receive_frags" symbols have been added to the kernel ABI whitelists.

BZ#702675

The "ipv6_ext_hdr", "lro_receive_frags", "lro_vlan_hwaccel_receive_frags", "netif_set_real_num_tx_queues", and "pci_find_ext_capability" symbols have been added to the kernel ABI whitelists. The only exception is "pci_find_ext_capability", which is not available for IBM System z.

BZ#703125

The "compat_alloc_user_space" symbol has been added to the kernel ABI whitelists.

BZ#730410

The "paca" symbol has been added to the kernel ABI whitelists for the 64-bit PowerPC architecture.

BZ#748520

The "dm_put_device", "enl_register_ops", "m_device_name", "m_unregister_target", "m_register_target", "m_table_get_mode", "m_table_get_md", "m_get_device", and "enl_register_family" symbols have been added to the kernel ABI whitelists.

Note: It is not necessary to install the kabi-whitelists package in order to use Driver Updates. The kabi-whitelists package only provides reference files for use by those creating Driver Update packages, or for those who wish to enable support for verification of kernel ABI compatibility by installing the appropriate Yum plug-in.

All users of kabi-whitelists are advised to upgrade to this updated package, which adds these enhancements.

4.113. KDEACCESSIBILITY

4.113.1. RHBA-2011:1173 — kdeaccessibility bug fix update

Updated kdeaccessibility packages that fix one bug are now available for Red Hat Enterprise Linux 6.

KDE is a graphical desktop environment for the X Window System. Kdeaccessibility contains KDE accessibility utilities, including KMouseTool (to initiate mouse clicks), KMag (to magnify parts of the screen), and KMouth & KTTS (a text-to-speech utility).

Bug Fix

BZ#587897

Prior to this update, the icon for the kttsmsg program incorrectly appeared in GNOME Application's Accessories menu. This bug has been fixed in this update so that the icon is now no longer displayed, as expected.

All users of kdeaccessibility are advised to upgrade to these updated packages, which fix this bug.

4.114. KDEADMIN

4.114.1. RHBA-2011:1117 — kdeadmin bug fix update

An updated kdeadmin package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The kdeadmin package contains administrative tools for the K Desktop Environment.

Bug Fixes

BZ#587904

Prior to this update, the icon for the ksystemlog program did not appear correctly in GNOME Application's System Tools menu. This bug has been fixed in this update so that the icon is now displayed as expected.

BZ#692737

Prior to this update, the Network Settings component that was included in KDE's System Settings was not compatible with NetworkManager in Red Hat Enterprise Linux 6. As a result, the spurious message "Your Platform is Not Supported" was displayed in the aforementioned component's dialog

window. Furthermore, no network interface controllers (NICs) were displayed in the dialog window. These problems have been resolved in this update by removing the Network Settings component from KDE's System Settings.

Users of kdeadmin are advised to upgrade to this updated package, which fixes these bugs.

4.115. KDEBASE

4.115.1. RHBA-2011:1200 — kdebase bug fix update

Updated kdebase packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The K Desktop Environment (KDE) is a graphical desktop environment for the X Window System. The kdebase package includes core applications for KDE.

Bug Fixes

BZ#631481

Prior to this update, when starting another instance of the konsole application in an already running konsole instance, the spurious "Undecodable sequence: \001b(hex)[?1034h" message was displayed. This bug has been fixed in this update and no longer occurs.

BZ#609039

Prior to this update, the System Settings application in KDE became unresponsive when entering a password in order to apply changes in the About Me dialog. With this update, the bug has been fixed so that entering a password works properly.

All users of kdebase are advised to upgrade to these updated packages, which fix these bugs.

4.116. KDEBASE-WORKSPACE

4.116.1. RHBA-2011:1115 — kdebase-workspace bug fix update

Updated kdebase-workspace packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

KDE is a graphical desktop environment for the X Window System. The kdebase-workspace packages contains utilities for basic operations with the desktop environment. It allows users for example, to change system settings, resize and rotate X screens or set panels and widgets on the workspace.

Bug Fixes

BZ#587917

If the KDE and GNOME desktop environments were both installed on one system, two System Monitor utilities were installed as well. These, located in System Tools of the Applications menu, had the same icons and title, which may have confused the user. With this update, KDE icons are used for the ksysguard tool.

BZ#639359

Prior to this update, the ksysguard process terminated unexpectedly with a segmentation fault after clicking the OK button in the Properties dialog of the Network History tab, which is included in the

ksysguard application. This bug has been fixed in this update so that ksysguard no longer crashes and works properly.

BZ#649345

Previously, when rebooting the system, the kdm utility terminated with a segmentation fault if auto-login was enabled. This was caused by a NULL password being sent to the master process, which has been fixed, and rebooting the system with auto-login enabled no longer causes kdm to crash.

BZ#666295

When clicking Help in the Battery Monitor Settings dialog of the Battery Monitor widget, the message "The file or folder help:/plasma-desktop/index.html does not exist" appeared instead of displaying the help pages. This update adds the missing help pages, which fixes the problem.

All users of kdebase-workspace are advised to upgrade to these updated packages, which fix these bugs.

4.117. KDEPIM-RUNTIME

4.117.1. RHBA-2011:1094 — kdepim-runtime bug fix update

Updated kdepim-runtime packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

KDE is a graphical desktop environment for the X Window System. The kdepim-runtime package contain the KDE PIM Runtime Environment.

Bug Fixes

BZ#660581

Prior to this update, it was not possible to build the kdepim-runtime package on Red Hat Enterprise Linux 6. This problem has been resolved in this update and no longer occurs.

BZ#625121

Prior to this update, Akonaditray, which is an application included in KDE, was incorrectly displayed in the GNOME Applications menu. This bug has been fixed in this update so that Akonaditray is no longer displayed in the aforementioned menu.

All users of kdepim-runtime are advised to upgrade to these updated packages, which fix these bugs.

4.118. KDEUTILS

4.118.1. RHBA-2011:1206 — kdeutils bug fix update

Updated kdeutils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

KDE is a graphical desktop environment for the X Window System. The kdeutils packages include several utilities for the KDE desktop environment.

Bug Fix

BZ#625116

Prior to this update, the icon for the Sweeper utility did not appear correctly in GNOME Application's Accessories menu. This bug has been fixed in this update so that the icon is now displayed as expected.

All users of kdeutils are advised to upgrade to these updated packages, which fix this bug.

4.119. KERNEL

4.119.1. RHSA-2013:1026 — Important: kernel security and bug fix update

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 6.2 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-1773, Important

A buffer overflow flaw was found in the way UTF-8 characters were converted to UTF-16 in the utf8s_to_utf16s() function of the Linux kernel's FAT file system implementation. A local user able to mount a FAT file system with the "utf8=1" option could use this flaw to crash the system or, potentially, to escalate their privileges.

CVE-2012-1796, Important

A flaw was found in the way KVM (Kernel-based Virtual Machine) handled guest time updates when the buffer the guest registered by writing to the MSR_KVM_SYSTEM_TIME machine state register (MSR) crossed a page boundary. A privileged guest user could use this flaw to crash the host or, potentially, escalate their privileges, allowing them to execute arbitrary code at the host kernel level.

CVE-2013-1797, Important

A potential use-after-free flaw was found in the way KVM handled guest time updates when the GPA (guest physical address) the guest registered by writing to the MSR_KVM_SYSTEM_TIME machine state register (MSR) fell into a movable or removable memory region of the hosting user-space process (by default, QEMU-KVM) on the host. If that memory region is deregistered from KVM using KVM_SET_USER_MEMORY_REGION and the allocated virtual memory reused, a privileged guest user could potentially use this flaw to escalate their privileges on the host.

CVE-2012-1798, Important

A flaw was found in the way KVM emulated IOAPIC (I/O Advanced Programmable Interrupt Controller). A missing validation check in the ioapic_read_indirect() function could allow a privileged guest user to crash the host, or read a substantial portion of host kernel memory.

CVE-2012-1848, Low

A format string flaw was found in the ext3_msg() function in the Linux kernel's ext3 file system implementation. A local user who is able to mount an ext3 file system could use this flaw to cause a denial of service or, potentially, escalate their privileges.

Red Hat would like to thank Andrew Honig of Google for reporting CVE-2013-1796, CVE-2013-1797, and CVE-2013-1798.

Bug Fixes

BZ#956294

The virtual file system (VFS) code had a race condition between the unlink and link system calls that allowed creating hard links to deleted (unlinked) files. This could, under certain circumstances, cause inode corruption that eventually resulted in a file system shutdown. The problem was observed in Red Hat Storage during rsync operations on replicated Gluster volumes that resulted in an XFS shutdown. A testing condition has been added to the VFS code, preventing hard links to deleted files from being created.

BZ#972578

Various race conditions that led to indefinite log reservation hangs due to xfsaild "idle" mode occurred in the XFS file system. This could lead to certain tasks being unresponsive; for example, the cp utility could become unresponsive on heavy workload. This update improves the Active Item List (AIL) pushing logic in xfsaild. Also, the log reservation algorithm and interactions with xfsaild have been improved. As a result, the aforementioned problems no longer occur in this scenario.

BZ#972597

When the Active Item List (AIL) becomes empty, the xfsaild daemon is moved to a task sleep state that depends on the timeout value returned by the xfsaild_push() function. The latest changes modified xfsaild_push() to return a 10-ms value when the AIL is empty, which sets xfsaild into the uninterruptible sleep state (D state) and artificially increased system load average. This update applies a patch that fixes this problem by setting the timeout value to the allowed maximum, 50 ms. This moves xfsaild to the interruptible sleep state (S state), avoiding the impact on load average.

BZ#972607

When adding a virtual PCI device, such as virtio disk, virtio net, e1000 or rtl8139, to a KVM guest, the kacpid thread reprograms the hot plug parameters of all devices on the PCI bus to which the new device is being added. When reprogramming the hot plug parameters of a VGA or QXL graphics device, the graphics device emulation requests flushing of the guest's shadow page tables. Previously, if the guest had a huge and complex set of shadow page tables, the flushing operation took a significant amount of time and the guest could appear to be unresponsive for several minutes. This resulted in exceeding the threshold of the "soft lockup" watchdog and the "BUG: soft lockup" events were logged by both, the guest and host kernel. This update applies a series of patches that deal with this problem. The KVM's Memory Management Unit (MMU) now avoids creating multiple page table roots in connection with processors that support Extended Page Tables (EPT). This prevents the guest's shadow page tables from becoming too complex on machines with EPT support. MMU now also flushes only large memory mappings, which alleviates the situation on machines where the processor does not support EPT. Additionally, a free memory accounting race that could prevent KVM MMU from freeing memory pages has been fixed.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.119.2. RHSA-2013:0741 — Important: kernel security and bug fix update

Updatedkernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 6.2 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages contain the Linux kernel.

Security Fixes

CVE-2013-0871, Important

A race condition was found in the way the Linux kernel's ptrace implementation handled PTRACE_SETREGS requests when the debuggee was woken due to a SIGKILL signal instead of being stopped. A local, unprivileged user could use this flaw to escalate their privileges.

CVE-2012-2133, Moderate

A use-after-free flaw was found in the Linux kernel's memory management subsystem in the way quota handling for huge pages was performed. A local, unprivileged user could use this flaw to cause a denial of service or, potentially, escalate their privileges.

Red Hat would like to thank Shachar Raindel for reporting CVE-2012-2133.

Bug Fixes

BZ#911265

The Intel 5520 and 5500 chipsets do not properly handle remapping of MSI and MSI-X interrupts. If the interrupt remapping feature is enabled on the system with such a chipset, various problems and service disruption could occur (for example, a NIC could stop receiving frames), and the "kernel: do_IRQ: 7.71 No irq handler for vector (irq -1)" error message appears in the system logs. As a workaround to this problem, it has been recommended to disable the interrupt remapping feature in the BIOS on such systems, and many vendors have updated their BIOS to disable interrupt remapping by default. However, the problem is still being reported by users without proper BIOS level with this feature properly turned off. Therefore, this update modifies the kernel to check if the interrupt remapping feature is enabled on these systems and to provide users with a warning message advising them on turning off the feature and updating the BIOS.

BZ#913161

A possible race between the n_tty_read() and reset_buffer_flags() functions could result in a NULL pointer dereference in the n_tty_read() function under certain circumstances. As a consequence, a kernel panic could have been triggered when interrupting a current task on a serial console. This update modifies the tty driver to use a spin lock to prevent functions from a parallel access to variables. A NULL pointer dereference causing a kernel panic can no longer occur in this scenario.

BZ#915581

Previously, running commands such as "ls", "find" or "move" on a MultiVersion File System (MVFS) could cause a kernel panic. This happened because the d_validate() function, which is used for dentry validation, called the kmem_ptr_validate() function to validate a pointer to a parent dentry. The pointer could have been freed anytime so the kmem_ptr_validate() function could not guarantee the pointer to be dereferenced, which could lead to a NULL pointer derefence. This update modifies d_validate() to verify the parent-child relationship by traversing the parent dentry's list of child dentries, which solves this problem. The kernel no longer panics in the described scenario.

BZ#921959

When running a high thread workload of small-sized files on an XFS file system, sometimes, the

system could become unresponsive or a kernel panic could occur. This occurred because the xfsaild daemon had a subtle code path that led to lock recursion on the xfsaild lock when a buffer in the AIL was already locked and an attempt was made to force the log to unlock it. This patch removes the dangerous code path and queues the log force to be invoked from a safe locking context with respect to xfsaild. This patch also fixes the race condition between buffer locking and buffer pinned state that exposed the original problem by rechecking the state of the buffer after a lock failure. The system no longer hangs and kernel no longer panics in this scenario.

BZ#922140

A race condition could occur between page table sharing and virtual memory area (VMA) teardown. As a consequence, multiple "bad pmd" message warnings were displayed and "kernel BUG at mm/filemap.c:129" was reported while shutting down applications that share memory segments backed by huge pages. With this update, the VM_MAYSHARE flag is explicitly cleaned during the unmap_hugepage_range() call under the i_mmap_lock. This makes VMA ineligible for sharing and avoids the race condition. After using shared segments backed by huge pages, applications like databases and caches shut down correctly, with no crash.

BZ#923849

Previously, the NFS Lock Manager (NLM) did not resend blocking lock requests after NFSv3 server reboot recovery. As a consequence, when an application was running on a NFSv3 mount and requested a blocking lock, the application received an -ENOLCK error. This patch ensures that NLM always resend blocking lock requests after the grace period has expired.

BZ#924836

A bug in the anon_vma lock in the mprotect() function could cause virtual memory area (vma) corruption. The bug has been fixed so that virtual memory area corruption no longer occurs in this scenario.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.119.3. RHBA-2012:1254 — kernel bug fix and enhancement update

Updated kernel packages that fix three bugs and add two enhancements are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Bug Fixes

BZ#846831

Previously, the TCP socket bound to NFS server contained a stale skb_hints socket buffer. Consequently, kernel could terminate unexpectedly. A patch has been provided to address this issue and skb_hints is now properly cleared from the socket, thus preventing this bug.

BZ#847041

On Intel systems with Pause Loop Exiting (PLE), or AMD systems with Pause Filtering (PF), it was possible for larger multi-CPU KVM guests to experience slowdowns and soft lock-ups. Due to a boundary condition in kvm_vcpu_on_spin, all the VCPUs could try to yield to VCPU0, causing contention on the run queue lock of the physical CPU where the guest's VCPU0 is running. This update eliminates the boundary condition in kvm_vcpu_on_spin.

BZ#847944

Due to a missing return statement, the nfs_attr_use_mounted_on_file() function returned a wrong value. As a consequence, redundant ESTALE errors could potentially be returned. This update adds the proper return statement to nfs_attr_use_mounted_on_file(), thus preventing this bug.

Enhancements

BZ#847732

This update adds support for the Proportional Rate Reduction (PRR) algorithms for the TCP protocol. This algorithm determines TCP's sending rate in fast recovery. PRR avoids excessive window reductions and improves accuracy of the amount of data sent during loss recovery. In addition, a number of other enhancements and bug fixes for TCP are part of this update.

BZ#849550

This update affects performance of the O_DSYNC flag on the GFS2 file system when only data (and not metadata such as file size) has been dirtied as a result of the write() system call. Prior to this update, write calls with O_DSYNC were behaving the same way as with O_SYNC at all times. With this update, O_DSYNC write calls only write back data if the inode's metadata is not dirty. This results in a considerable performance improvement for this specific case. Note that the issue does not affect data integrity. The same issue also applies to the pairing of the write() and fdatasync() system calls.

All users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. The system must be rebooted for this update to take effect.

4.119.4. RHBA-2012:1198 — kernel bug fix update

Updated kernel packages that fix two bugs are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

When an NTP server asserts the STA_INS flag (Leap Second Insert), the kernel starts an hrtimer (high-resolution timer) with a countdown clock. This hrtimer expires at end of the current month, midnight UTC, and inserts a second into the kernel timekeeping structures. A scheduled leap second occurred on June 30 2012 midnight UTC.

Bug Fixes

BZ#840949

Previously in the kernel, when the leap second hrtimer was started, it was possible that the kernel livelocked on the xtime_lock variable. This update fixes the problem by using a mixture of separate subsystem locks (timekeeping and ntp) and removing the xtime_lock variable, thus avoiding the livelock scenarios that could occur in the kernel.

BZ#847365

After the leap second was inserted, applications calling system calls that used futexes consumed almost 100% of available CPU time. This occurred because the kernel's timekeeping structure update did not properly update these futexes. The futexes repeatedly expired, re-armed, and then expired immediately again. This update fixes the problem by properly updating the futex expiration times by calling the clock_was_set_delayed() function, an interrupt-safe method of the clock_was_set() function.

All users are advised to upgrade to these updated packages, which fix these bugs. The system must be rebooted for this update to take effect.

4.119.5. RHBA-2013:0184 — kernel bug fix update

Updated kernel packages that fix three bugs are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Bug Fixes

BZ#880083

Previously, the IP over Infiniband (IPoIB) driver maintained state information about neighbors on the network by attaching it to the core network's neighbor structure. However, due to a race condition between the freeing of the core network neighbor struct and the freeing of the IPoIB network struct, a use after free condition could happen, resulting in either a kernel oops or 4 or 8 bytes of kernel memory being zeroed when it was not supposed to be. These patches decouple the IPoIB neighbor struct from the core networking stack's neighbor struct so that there is no race between the freeing of one and the freeing of the other.

BZ#884421

Previously, the HP Smart Array, or hpsa, driver used target reset. However, HP Smart Array logical drives do not support target reset. Therefore, if the target reset failed, the logical drive was taken offline with a file system error. The hpsa driver has been updated to use LUN reset instead of target reset, which is supported by these drives.

BZ#891563

Previously, the xdr routines in NFS version 2 and 3 conditionally updated the res->count variable. Read retry attempts after a short NFS read() call could fail to update the res->count variable, resulting in truncated read data being returned. With this update, the res->count variable is updated unconditionally, thus preventing this bug.

Users should upgrade to these updated packages, which contain backported patches to fix these bugs. The system must be rebooted for this update to take effect.

4.119.6. RHSA-2011:1530 — Moderate: Red Hat Enterprise Linux 6.2 kernel security, bug fix, and enhancement update

Updated kernel packages that fix multiple security issues, address several hundred bugs, and add numerous enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 6. This is the second regular update.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2011-1020, Moderate

The proc file system could allow a local, unprivileged user to obtain sensitive information or possibly cause integrity issues.

CVE-2011-3347, Moderate

Non-member VLAN (virtual LAN) packet handling for interfaces in promiscuous mode and also using the **be2net** driver could allow an attacker on the local network to cause a denial of service.

CVE-2011-3638, Moderate

A flaw was found in the Linux kernel in the way splitting two extents in **ext4_ext_convert_to_initialized()** worked. A local, unprivileged user with access to mount and unmount ext4 file systems could use this flaw to cause a denial of service.

CVE-2011-4110, Moderate

A NULL pointer dereference flaw was found in the way the Linux kernel's key management facility handled user-defined key types. A local, unprivileged user could use the keyctl utility to cause a denial of service.

Red Hat would like to thank Kees Cook for reporting CVE-2011-1020; Somnath Kotur for reporting CVE-2011-3347; and Zheng Liu for reporting CVE-2011-3638.

Bug Fixes

BZ#713682

When a host was in recovery mode and a SCSI scan operation was initiated, the scan operation failed and provided no error output. This bug has been fixed and the SCSI layer now waits for recovery of the host to complete scan operations for devices.

BZ#712139

In a GFS2 file system, when the responsibility for deallocation was passed from one node to another, the receiving node may not have had a fully up-to-date inode state. If the sending node has changed the important parts of the state in the mean time (block allocation/deallocation) then this resulted in triggering an assert during the deallocation on the receiving node. With this update, the inode state is refreshed correctly during deallocation on the receiving node, ensuring that deallocation proceeds normally.

BZ#712131

Issues for which a host had older hypervisor code running on newer hardware, which exposed the new CPU features to the guests, were discovered. This was dangerous because newer guest kernels (such as Red Hat Enterprise Linux 6) may have attempted to use those features or assume certain machine behaviors that it would not be able to process because it was, in fact, a Xen guest. One such place was the intel_idle driver which attempts to use the MWAIT and MONITOR instructions. These instructions are invalid operations for a Xen PV guest. This update provides a patch, which masks the MWAIT instruction to avoid this issue.

BZ#712102

The 128-bit multiply operation in the pvclock.h function was missing an output constraint for EDX which caused a register corruption to appear. As a result, Red Hat Enterprise Linux 3.8 and Red Hat Enterprise Linux 3.9 KVM guests with a Red Hat Enterprise Linux 6.1 KVM host kernel exhibited time inconsistencies. With this update, the underlying source code has been modified to address this issue, and time runs as expected on the aforementioned systems.

BZ#712000

Prior to this update, the following message appeared in kernel log files:

```
[bnx2x_extract_max_cfg:1079(eth11)]Illegal configuration detected for
Max BW - using 100 instead
```

The above message appeared on bnx2x interfaces in the multi-function mode which were not used and had no link, thus, not indicating any actual problems with connectivity. With this update, the message has been removed and no longer appears in kernel log files.

BZ#713730

Previously, some enclosure devices with a broken firmware reported incorrect values. As a consequence, kernel sometimes terminated unexpectedly. A patch has been provided to address this issue, and the kernel crashes no longer occur even if an enclosure device reports incorrect or duplicate data.

BZ#709856

Xen guests cannot make use of all CPU features, and in some cases they are even risky to be advertised. One such feature is CONSTANT_TSC. This feature prevents the TSC (Time Stamp Counter) from being marked as unstable, which allows the sched_clock_stable option to be enabled. Having the sched_clock_stable option enabled is problematic for Xen PV guests because the sched_clock() function has been overridden with the xen_sched_clock() function, which is not synchronized between virtual CPUs. This update provides a patch, which sets all x86_power features to 0 as a preventive measure against other potentially dangerous assumptions the kernel could make based on the features, fixing this issue.

BZ#623712

RHEL6.2 backported the scalability improvement on creating many 'cpu' control groups (cgroups) on a system with a large number of CPUs. The creation process for large number of cgroups will no longer hog the machine when the control groups feature is enabled.

In addition to the scalability improvement, a /proc tunable parameter, dd sysctl_sched_shares_window, has been added, and the default is set to 10 ms.

BZ#719304

Older versions of be2net cards firmware may not recognize certain commands and return illegal/unsupported errors, causing confusing error messages to appear in the logs. With this update, the driver handles these errors gracefully and does not log them.

BZ#722461

On IBM System z, if a Linux instance with large amounts of anonymous memory runs into a memory shortage the first time, all pages on the active or inactive lists are considered referenced. This causes the memory management on IBM System z to do a full check over all page cache pages and start writeback for all of them. As a consequence, the system became temporarily unresponsive when the described situation occurred. With this update, only pages with active mappers are checked and the page scan now does not cause the hangs.

BZ#722596

This update fixes the inability of the be2net driver to work in a kdump environment. It clears an interrupt bit (in the card) that may be set while the driver is probed by the kdump kernel after a crash.

BZ#705441

A previously introduced update intended to prevent IOMMU (I/O Memory Management Unit) domain exhaustion introduced two regressions. The first regression was a race where a domain pointer could be freed while a lazy flush algorithm still had a reference to it, eventually causing kernel panic. The second regression was an erroneous reference removal for identity mapped and VM IOMMU domains, causing I/O errors. Both of these regressions could only be triggered on Intel based platforms, supporting VT-d, booted with the intel_iommu=on boot option. With this update, the underlying source code of the intel-iommu driver has been modified to resolve both of these problems. A forced flush is now used to avoid the lazy use after free issue, and extra checks have been added to avoid the erroneous reference removal.

BZ#635596

This update fixes two bugs related to Rx checksum offloading. These bugs caused a data corruption transferred over r8169 NIC when Rx checksum offloading was enabled.

BZ#704401

Prior to this update, kdump failed to create a vmcore file after triggering a crash on POWER7 systems with Dynamic DMA Windows enabled. This update provides a number of fixes that address this issue.

BZ#703935

Previously, auditing system calls used a simple check to determine whether a return value was positive or negative, which also determined the success of the system call. With an exception of few, this worked on most platforms and with most system calls. For example, the 32 bit mmap system call on the AMD64 architecture could return a pointer which appeared to be of value negative even though pointers are normally of unsigned values. This resulted in the success field being incorrect. This patch fixes the success field for all system calls on all architectures.

BZ#703245

When VLANs stacked on top of multiqueue devices passed through these devices, the queue_mapping value was not properly decremented because the VLAN devices called the physical devices via the ndo_select_queue method. This update removes the multiqueue functionality, resolving this issue.

BZ#703055

Prior to this update, Red Hat Enterprise Linux Xen (up to version 5.6) did not hide 1 GB pages and RDTSCP (enumeration features of CPUID), causing guest soft lock ups on AMD hosts when the guest's memory was greater than 8 GB. With this update, a Red Hat Enterprise Linux 6 HVM (Hardware Virtual Machine) guest is able to run on Red Hat Enterprise Linux Xen 5.6 and lower.

BZ#702742

Prior to this update, code was missing from the netif_set_real_num_tx_queues() function which prevented an increment of the real number of TX queues (the real_num_tx_queues value). This update adds the missing code; thus, resolving this issue.

BZ#725711

Previously, the inet6_sk_generic() function was using the obj_size variable to compute the address of its inner structure, causing memory corruption. With this update, the sk_alloc_size() is called every time there is a request for allocation, and memory corruption no longer occurs.

BZ#702057

Multiple GFS2 nodes attempted to unlink, rename, or manipulate files at the same time, causing various forms of file system corruption, panics, and withdraws. This update adds multiple checks for dinode's i_nlink value to assure inode operations such as link, unlink, or rename no longer cause the aforementioned problems.

BZ#701951

A kernel panic in the mpt2sas driver could occur on an IBM system using a drive with SMART (Self-Monitoring, Analysis and Reporting Technology) issues. This was because the driver was sending an SEP request while the kernel was in the interrupt context, causing the driver to enter the sleep state. With this update, a fake event is not executed from the interrupt context, assuring the SEP request is properly issued.

BZ#700538

When using certain SELinux policies, such as the MLS policy, it was not possible to properly mount the cgroupfs file system due to the way security checks were applied to the new cgroupfs inodes during the mount operation. With this update, the security checks applied during the mount operation have been changed so that they always succeed, and the cgroupfs file system can now be successfully mounted and used with the MLS SELinux policy. This issue did not affect systems which used the default targeted policy.

BZ#729220

When a SCTP (Stream Control Transmission Protocol) packet contained two COOKIE_ECHO chunks and nothing else, the SCTP state machine disabled output processing for the socket while processing the first COOKIE_ECHO chunk, then lost the association and forgot to re-enable output processing for the socket. As a consequence, any data which needed to be sent to a peer were blocked and the socket appeared to be unresponsive. With this update, a new SCTP command has been added to the kernel code, which sets the association explicitly; the command is used when processing the second COOKIE_ECHO chunk to restore the context for SCTP state machine, thus fixing this bug.

BZ#698268

The hpsa driver has been updated to provide a fix for hpsa driver kdump failures.

BZ#696777

Prior to this update, interrupts were enabled before the dispatch log for the boot CPU was set up, causing kernel panic if a timer interrupt occurred before the log was set up. This update adds a check to the scan_dispatch_log function to ensure the dispatch log has been allocated.

BZ#696754

Prior to this update, the interrupt service routine was performing unnecessary MMIO operation during performance testing on IBM POWER7 machines. With this update, the logic of the routine has been modified so that there are fewer MMIO operations in the performance path of the code. Additionally, as a result of the aforementioned change, an existing condition was exposed where the IPR driver (the controller device driver) could return an unexpected HRRQ (Host Receive Request) interrupt. The original code flagged the interrupt as unexpected and then reset the adapter. After further analysis, it was confirmed that this condition could occasionally occur and the interrupt can be safely ignored. Additional code provided by this update detects this condition, clears the interrupt, and allows the driver to continue without resetting the adapter.

BZ#732706

The ACPI (Advanced Control and Power Interface) core places all events to the kacpi_notify queue including PCI hotplug events. When the acpiphp driver was loaded and a PCI card with a PCI-to-PCI bridge was removed from the system, the code path attempted to empty the kacpi_notify queue

which causes a deadlock, and the kacpi_notify thread became unresponsive. With this update, the call sequence has been fixed, and the bridge is now cleaned-up properly in the described scenario.

BZ#669363

Prior to this update, the /proc/diskstats file showed erroneous values. This occurred when the kernel merged two I/O operations for adjacent sectors which were located on different disk partitions. Two merge requests were submitted for the adjacent sectors, the first request for the second partition and the second request for the first partition, which was then merged to the first request. The first submission of the merge request incremented the in_flight value for the second partition. However, at the completion of the merge request, the in_flight value of a different partition (the first one) was decremented. This resulted in the erroneous values displayed in the /proc/diskstats file. With this update, the merging of two I/O operations which are located on different disk partitions has been fixed and works as expected.

BZ#670765

Due to an uninitialized variable (specifically, the isr_ack variable), a virtual guest could become unresponsive when migrated while being rebooted. With this update, the said variable is properly initialized, and virtual guests no longer hang in the aforementioned scenario.

BZ#695231

Prior to this update, the be2net driver was using the BE3 chipset in legacy mode. This update enables this chipset to work in a native mode, making it possible to use all 4 ports on a 4-port integrated NIC.

BZ#694747

A Windows Server 2008 32-bit guest installation failed on a Red Hat Enterprise Linux 6.1 Snap2 KVM host when allocating more than one virtual CPU (vcpus > 1) during the installation. As soon the installation started after booting from ISO, a blue screen with the following error occurred:

```
A problem has been detected and windows has been shut down to prevent
damage to your computer.
```

This was because a valid microcode update signature was not reported to the guest. This update fixes this issue by reporting a non-zero microcode update signature to the guest.

BZ#679526

Disk read operations on a memory constrained system could cause allocations to stall. As a result, the system performance would drop considerably. With this update, latencies seen in page reclaim operations have been reduced and their efficiency improved; thus, fixing this issue.

BZ#736667

A workaround to the megaraid_sas driver was provided to address an issue but as a side effect of the workaround, megaraid_sas stopped to report certain enclosures, CD-ROM drives, and other devices. The underlying problem for the issue has been fixed as reported in BZ#741166. With this update, the original workaround has been reverted, and megaraid_sas now reports many different devices as before.

BZ#694210

This update fixes a regression in which a client would use an UNCHECKED NFS CREATE call when an open system call was attempted with the O_EXCL|O_CREAT flag combination. An EXCLUSIVE NFS CREATE call should have been used instead to ensure that O_EXCL semantics were

preserved. As a result, an application could be led to believe that it had created the file when it was in fact created by another application.

BZ#692167

A race between the FSFREEZE ioctl() command to freeze an ext4 file system and mmap I/O operations would result in a deadlock if these two operations ran simultaneously. This update provides a number of patches to address this issue, and a deadlock no longer occurs in the previously-described scenario.

BZ#712653

When a CPU is about to modify data protected by the RCU (Read Copy Update) mechanism, it has to wait for other CPUs in the system to pass a quiescent state. Previously, the guest mode was not considered a quiescent state. As a consequence, if a CPU was in the guest mode for a long time, another CPU had to wait a long time in order to modify RCU-protected data. With this update, the rcu_virt_note_context_switch() function, which marks the guest mode as a quiescent state, has been added to the kernel, thus resolving this issue.

BZ#683658

The patch that fixed BZ#556572 introduced a bug where the page lock was being released too soon, allowing the do_wp_page function to reuse the wrprotected page before PageKsm would be set in page->mapping. With this update, a new version of the original fix was introduced, thus fixing this issue.

BZ#738110

Due to the partial support of IPv6 multicast snooping, IPv6 multicast packets may have been dropped. This update fixes IPv6 multicast snooping so that packets are no longer dropped.

BZ#691310

While executing a multi-threaded process by multiple CPUs, page-directory-pointer-table entry (PDPTE) registers were not fully flushed from the CPU cache when a Page Global Directory (PGD) entry was changed in x86 Physical Address Extension (PAE) mode. As a consequence, the process failed to respond for a long time before it successfully finished. With this update, the kernel has been modified to flush the Translation Lookaside Buffer (TLB) for each CPU using a page table that has changed. Multi-threaded processes now finish without hanging.

BZ#738379

When a kernel NFS server was being stopped, kernel sometimes terminated unexpectedly. A bug has been fixed in the wait_for_completion_interruptible_timeout() function and the crashes no longer occur in the described scenario.

BZ#690745

Recent Red Hat Enterprise Linux 6 releases use a new naming scheme for network interfaces on some machines. As a result, the installer may use different names during an upgrade in certain scenarios (typically em1 is used instead of eth0 on new Dell machines). However, the previously used network interface names are preserved on the system and the upgraded system will still use the previously used interfaces. This is not the case for Yum upgrades.

BZ#740465

A scenario for this bug involves two hosts, configured to use IPv4 network, and two guests, configured to use IPv6 network. When a guest on host A attempted to send a large UDP datagram to host B, host A terminated unexpectedly. With this update, the ipv6_select_ident() function has been

fixed to accept the in6_addr parameter and to use the destination address in IPv6 header when no route is attached, and the crashes no longer occur in the described scenario.

BZ#693894

Migration of a Windows XP virtual guest during the early stage of a boot caused the virtual guest OS to fail to boot correctly. With this update, the underlying source code has been modified to address this issue, and the virtual guest OS no longer fails to boot.

BZ#694358

This update adds a missing patch to the ixgbe driver to use the kernel's generic routine to set and obtain the DCB (Data Center Bridging) priority. Without this fix, applications could not properly query the DCB priority.

BZ#679262

In Red Hat Enterprise Linux 6.2, due to security concerns, addresses in /proc/kallsyms and /proc/modules show all zeros when accessed by a non-root user.

BZ#695859

Red Hat Enterprise Linux 6.0 and 6.1 defaulted to running UEFI systems in a physical addressing mode. Red Hat Enterprise Linux 6.2 defaults to running UEFI systems in a virtual addressing mode. The previous behavior may be obtained by passing the physefi kernel parameter.

BZ#695966

After receiving an ABTS response, the FCoE (Fibre Channel over Ethernet) DDP error status was cleared. As a result, the FCoE DDP context invalidation was incorrectly bypassed and caused memory corruption. With this update, the underlying source code has been modified to address this issue, and memory corruption no longer occurs.

BZ#696511

Suspending a system to RAM and consequently resuming it caused USB3.0 ports to not work properly. This was because a USB3.0 device configured for MSIX would, during the resume operation, incorrectly read its previous interrupt state. This would lead it to fall back to a legacy mode and appear unresponsive. With this update, the interrupt state is cached, allowing the driver to properly resume its previous state.

BZ#662666

Deleting the lost+found directory on a file system with inodes of size greater than 128 bytes and reusing inode 11 for a different file caused the extended attributes for inode 11 (which were set before a umount operation) to not be saved after a file system remount. As a result, the extended attributes were lost after the remount. With this update, inodes store their extended attributes under all circumstances.

BZ#698023

Prior to this update, in the __cache_alloc() function, the ac variable could be changed after cache_alloc_refill() and the following kmemleak_erase() function could receive an incorrect pointer, causing kernel panic. With this update, the ac variable is updated after the cache_alloc_refill() unconditionally.

BZ#698625

This update includes two fixes for the bna driver, specifically:

- A memory leak was caused by an unintentional assignment of the NULL value to the RX path destroy callback function pointer after a correct initialization.
- During a kernel crash, the bna driver control path state machine and firmware did not receive a notification of the crash, and, as a result, were not shut down cleanly.

BZ#700165

When an event caused the ibmvscsi driver to reset its CRQ, re-registering the CRQ returned H_CLOSED, indicating that the Virtual I/O Server was not ready to receive commands. As a consequence, the ibmvscsi driver offlined the adapter and did not recover. With this update, the interrupt is re-enabled after the reset so that when the Virtual I/O server is ready and sends a CRQ init, it is able to receive it and resume initialization of the VSCSI adapter.

BZ#700299

This update standardizes the printed format of UUIDs (Universally Unique Identifier)/GUIDs (Globally Unique Identifier) by using an additional extension to the %p format specifier (which is used to show the memory address value of a pointer).

BZ#702036

Prior to this update, the ehea driver caused a kernel oops during a memory hotplug if the ports were not up. With this update, the waitqueues are initialized during the port probe operation, instead of during the port open operation.

BZ#702263

While running gfs2_grow, the file system became unresponsive. This was due to the log not getting flushed when a node dropped its rindex glock so that another node could grow the file system. If the log did not get flushed, GFS2 could corrupt the sd_log_le_rg list, ultimately causing a hang. With this update, a log flush is forced when the rindex glock is invalidated; gfs2_grow completes as expected and the file system remains accessible.

BZ#703251

The Brocade BFA FC/FCoE driver was previously selectively marked as a Technology Preview based on the type of the adapter. With this update, the Brocade BFA FC/FCoE driver is always marked as a Technology Preview.

BZ#703265

The Brocade BFA FC SCSI driver (bfa driver) has been upgraded to version 2.3.2.4. Additionally, this update provides the following two fixes:

- A firmware download memory leak was caused by the release_firmware() function not being called after the request_firmware() function. Similarly, the firmware download interface has been fixed and now works as expected.
- During a kernel crash, the bfa I/O control state machine and firmware did not receive a notification of the crash, and, as a result, were not shut down cleanly.

BZ#704231

A previously released patch for BZ#625487 introduced a kABI (Kernel Application Binary Interface) workaround that extended struct sock (the network layer representation of sockets) by putting the extension structure in the memory right after the original structure. As a result, the prot->obj_size pointer had to be adjusted in the proto_register function. Prior to this update, the adjustment was done only if the alloc_slab parameter of the proto_register function was not 0. When the alloc_slab

parameter was 0, drivers performed allocations themselves using sk_alloc and as the allocated memory was lower than needed, a memory corruption could occur. With this update, the underlying source code has been modified to address this issue, and a memory corruption no longer occurs.

BZ#705082

A scalability issue with KVM/QEMU was discovered in the idr_lock spinlock in the posix-timers code, resulting in excessive CPU resource usage. With this update, the underlying source code has been modified to address this issue, and the aforementioned spinlock no longer uses excessive amounts of CPU resources.

BZ#723650

When a NFS server returned more than two GETATTR bitmap words in response to the FATTR4_ACL attribute request, decoding operations of the nfs4_getfacl() function failed. A patch has been provided to address this issue and the ACLs are now returned in the described scenario.

BZ#707268

After hot plugging one of the disks of a non-boot 2-disk RAID1 pair, the md driver would enter an infinite resync loop thinking there was a spare disk available, when, in fact, there was none. This update adds an additional check to detect the previously mentioned situation; thus, fixing this issue.

BZ#707757

The default for CFQ's group_isolation variable has been changed from 0 to 1 (/sys/block/<device>/queue/iosched/group_isolation). After various testing and numerous user reports, it was found that having default 1 is more useful. When set to 0, all random I/O queues become part of the root cgroup and not the actual cgroup which the application is part of. Consequently, this leads to no service differentiation for applications.

BZ#691945

In error recovery, most SCSI error recovery stages send a TUR (Test Unit Ready) command for every bad command when a driver error handler reports success. When several bad commands pointed to a same device, the device was probed multiple times. When the device was in a state where the device did not respond to commands even after a recovery function returned success, the error handler had to wait for the commands to time out. This significantly impeded the recovery process. With this update, SCSI mid-layer error routines to send test commands have been fixed to respond once per device instead of once per bad command, thus reducing error recovery time considerably.

BZ#696396

Prior to this update, loading the FS-Cache kernel module would cause the kernel to be tainted as a Technology Preview via the mark_tech_preview() function, which would cause kernel lock debugging to be disabled by the add_taint() function. However, the NFS and CIFS modules depend on the FS-Cache module so using either NFS or CIFS would cause the FS-Cache module to be loaded and the kernel tainted. With this update, FS-Cache only taints the kernel when a cache is brought online (for instance by starting the cachefilesd service) and, additionally, the add_taint() function has been modified so that it does not disable lock debugging for informational-only taints.

BZ#703728

This update removes temporary and unneeded files that were previously included with the kernel source code.

BZ#632802

Previously removed flushing of MMU updates in the kmap_atomic() and kunmap_atomic() functions

resulted in a dereference bug when processing a fork() under a heavy load. This update fixes page table entries in the kmap_atomic() and kunmap_atomic() functions to be synchronous, regardless of the lazy_mmu mode, thus fixing this issue.

BZ#746570

Previously fixed ABI issues in Red Hat Enterprise Linux 6.2 resulted in broken drivers that were built against the Red Hat Enterprise Linux 6.1 sources. This update adds padding to the net_device private structure so that the overruns resulting from an excessively-long pointer computed in the netdev_priv structure do not exceed the bounds of allocated memory.

BZ#737753

A previously introduced patch increased the value of the cpuid field from 8 to 16 bits. As a result, in some cases, modules built against the Red Hat Enterprise Linux 6.0 kernel source panicked when loaded into the new Red Hat Enterprise Linux 6.2 kernel. This update provides a patch which fixes this guaranteed backwards compatibility.

BZ#745253

KABI issues with additional fields in the "uv_blade_info" structure were discovered that prevented existing SGI modules from loading against the Red Hat Enterprise Linux 6.2 kernel. This update fixes the code in the "uv_blade_info" structure, and SGI modules load against the Red Hat Enterprise Linux 6.2 kernel as expected.

BZ#748503

Incorrect duplicate MAC addresses were being used on a rack network daughter card that contained a quad-port Intel I350 Gigabit Ethernet Controller. With this update, the underlying source code has been modified to address this issue, and correct MAC addresses are now used under all circumstances.

BZ#728676

Prior to this update, on certain HP systems, the hpsa and cciss drivers could become unresponsive and cause the system to crash when booting due to an attempt to read from a write-only register. This update fixes this issue, and the aforementioned crashes no longer occur.

BZ#693930

The cxgb4 driver never waited for RDMA_WR/FINI completions because the condition variable used to determine whether the completion happened was never reset, and this condition variable was reused for both connection setup and teardown. This caused various driver crashes under heavy loads because resources were released too early. With this update, atomic bits are used to correctly reset the condition immediately after the completion is detected.

BZ#710497

If a Virtual I/O server failed in a dual virtual I/O server multipath configuration, not all remote ports were deleted, causing path failover to not work properly. With this update, all remote ports are deleted so that path failover works as expected. For a single path configuration, the remote ports will enter the devloss state.

BZ#713868

When using the "crashkernel=auto" parameter and the "crashk_res.start" variable was set to 0, the existing logic automatically set the value of the "crashk_res.start" variable to 32M. However, to keep enough space in the RMO region for the first stage kernel on 64-bit PowerPC, the "crashk_res.start"

should have been set to KDUMP_KERNELBASE (64M). This update fixes this issue and properly assigns the correct value to the "crashk_res.start" variable.

BZ#743959

Due to a delay in settling of the usb-storage driver, the kernel failed to report all the disk drive devices in time to Anaconda, when booted in Unified Extensible Firmware Interface (UEFI) mode. Consequently, Anaconda presumed that no driver disks were available and loaded the standard drivers. With this update, both Anaconda and the driver use a one second delay, all devices are enumerated and inspected for driver disks properly.

BZ#690129

Prior to this update, the remap_file_pages() call was disabled for mappings without the VM_CAN_NONLINEAR flag set. Shared mappings of temporary file storage facilities (tmpfs) had this flag set but the flag was not set for the shared mappings of the /dev/zero device or shared anonymous mappings. With this update, the code has been modified and the VM_CAN_NONLINEAR flag is set also on the shared mappings of the /dev/zero device and shared anonymous mappings.

BZ#694309

The NFS client iterates through individual elements of a vector and issues a write request for each element to the server when the writev() function is called on a file opened with the O_DIRECT flag. Consequently, the server commits each individual write to the disk before replying to the client and the request transfer for the NFS client to the NFS server causes performance problems. With this update, the larger I/Os from the client are submitted only if all buffers are page-aligned, each individual vector element is aligned and has multiple pages, and the total I/O size is less than wsize (write block size).

BZ#699042

Improper shutdown in the e1000e driver caused a client with Intel 82578DM Gigabit Ethernet PHY to ignore the Wake-on-LAN signal and attempt to boot the client failed. This update applies the upstream Intel patch which fixes the problem.

BZ#703357

The "ifconfig up" command allocates memory for Direct Memory Access (DMA) operations. The memory is released when the "ifconfig down" command is issued. Previously, if another "ifconfig up" command was issued after an ifconfig up/down session, it re-enabled the DMA operations before sending the new DMA memory address to the NIC and the NIC could access the DMA address allocated during the previous ifconfig up/down session. However, the DMA address was already freed and could be used by another process. With this update, the underlying code has been modified and the problem no longer occurs.

BZ#729737

The in-process I/O operations of the Chelsio iWARP (cxgb3) driver could attempt to access a control data structure, which was previously freed after a hardware error that disabled the offload functionality occurred. This caused the system to terminate unexpectedly. With this update, the driver delays the freeing of the data structure and the problem no longer occurs.

BZ#734509

Previously, the capabilities flag of the WHEA_OSC call was set to 0. This could cause certain machines to disable APEI (ACPI Platform Error Interface). The flag is now set to 1, which enables APEI and fixes the problem.

BZ#748441

Previously, the origin device was being read when overwriting a complete chunk in the snapshot. This led to a significant memory leak when using the dm-snapshot module. With this update, reading of the origin device is skipped, and the memory leak no longer occurs.

BZ#750208

When the user attempted to list the mounted GFS2 file systems, a kernel panic occurred. This happened if the file in the location which the user tried to list was at the same time being manipulated by using the "fallocate" command. With this update, page cache is no longer used; the block is zeroed out at allocation time instead. Now, a kernel panic no longer occurs.

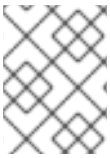
BZ#749018

The queuecommand error-handling function could cause memory leaks or prevent the TUR command from finishing for SCSI device drivers that enabled the support for lockless dispatching (lockless=1). This happened because the device driver did not call the scsi_cmd_get_serial() function and the serial_number property of the command remained zero. Consequently, the SCSI command could not be finished or aborted as the error-handling function always returned success for "serial_number == 0". The check for the serial number has been removed and the SCSI command can be finished or aborted.

BZ#750583

A previous patch for the Ironlake graphics controller and memory controller hub (GMCH) with a workaround for Virtualization Technology for Directed I/O (VT-d) introduced recursive calls to the unmap() function. With this update, a flag, which prevents the recursion, was added to the call chain, which allows the called routines to prevent the recursion.

Enhancements



NOTE

For more information on the most important of the RHEL 6.2 kernel enhancements, refer to the Red Hat Enterprise Linux 6.2 Release Notes.

BZ#707287

This update introduces a kernel module option that allows the disabling of the Flow Director.

BZ#706167

This update adds XTS (XEX-based Tweaked CodeBook) AES256 self-tests to meet the FIPS-140 requirements.

BZ#635968

This update introduces parallel port printer support for Red Hat Enterprise Linux 6.

BZ#699865

This update reduces the overhead of probes provided by kprobe (a dynamic instrumentation system), and enhances the performance of SystemTap.

BZ#696695

With this update, the JSM driver has been updated to support for enabling the Bell2 (with PLX chip) 2-port adapter on POWER7 systems. Additionally, EEH support has been added for to JSM driver.

BZ#669739

Memory limit for x86_64 domU PV guests has been increased to 128 GB: CONFIG_XEN_MAX_DOMAIN_MEMORY=128.

BZ#662208

In Red Hat Enterprise Linux 6.2, the taskstat utility (which prints ASET tasks status) in the kernel has been enhanced by the providing microsecond CPU time granularity to the top utility.

BZ#708365

Red Hat Enterprise Linux 6.2 introduced the multi-message send syscall, which is the send version of the existing recvmmsg syscall in Red Hat Enterprise Linux 6.

The following is the syscall sendmmsg socket API:

```
struct mmsghdr {
struct msghdr msg_hdr;
unsigned msg_len;
};

ssize_t sendmmsg(int socket, struct mmsghdr *datagrams, int vlen, int
flags);
```

BZ#647700

Red Hat Enterprise Linux 6.2's EDAC driver support for the latest Intel chipset is available as a Technical Preview.

BZ#599054

In Red Hat Enterprise Linux 6.2, the ipset feature in the kernel is added to store multiple IP addresses or port numbers, and match against the collection by iptables.

Users should upgrade to these updated packages, which contain backported patches to correct these issues, fix these bugs, and add these enhancement. The system must be rebooted for this update to take effect.

4.119.7. RHSA-2011:1849 — Important: kernel security and bug fix update

Updated kernel packages that fix one security issue and various bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2011-4127, Important

Using the SG_IO IOCTL to issue SCSI requests to partitions or LVM volumes resulted in the requests being passed to the underlying block device. If a privileged user only had access to a single partition or LVM volume, they could use this flaw to bypass those restrictions and gain read and write access (and be able to issue other SCSI commands) to the entire block device.

In KVM (Kernel-based Virtual Machine) environments using raw format virtio disks backed by a partition or LVM volume, a privileged guest user could bypass intended restrictions and issue read and write requests (and other SCSI commands) on the host, and possibly access the data of other guests that reside on the same underlying block device. Partition-based and LVM-based storage pools are not used by default. Refer to Red Hat Bugzilla bug 752375 for further details and a mitigation script for users who cannot apply this update immediately.

Bug Fixes

BZ#750459

Previously, idle load balancer kick requests from other CPUs could be serviced without first receiving an inter-processor interrupt (IPI). This could have led to a deadlock.

BZ#751403

This update fixes a performance regression that may have caused processes (including KVM guests) to hang for a number of seconds.

BZ#755545

When md_raid1_unplug_device() was called while holding a spinlock, under certain device failure conditions, it was possible for the lock to be requested again, deeper in the call chain, causing a deadlock. Now, md_raid1_unplug_device() is no longer called while holding a spinlock.

BZ#756426

In hpet_next_event(), an interrupt could have occurred between the read and write of the HPET (High Performance Event Timer) and the value of HPET_COUNTER was then beyond that being written to the comparator (HPET_Tn_CMP). Consequently, the timers were overdue for up to several minutes. Now, a comparison is performed between the value of the counter and the comparator in the HPET code. If the counter is beyond the comparator, the "-ETIME" error code is returned.

BZ#756427

Index allocation in the virtio-blk module was based on a monotonically increasing variable "index". Consequently, released indexes were not reused and after a period of time, no new were available. Now, virtio-blk uses the ida API to allocate indexes.

BZ#757671

A bug related to Context Caching existed in the Intel IOMMU support module. On some newer Intel systems, the Context Cache mode has changed from previous hardware versions, potentially exposing a Context coherency race. The bug was exposed when performing a series of hot plug and unplug operations of a Virtual Function network device which was immediately configured into the network stack, i.e., successfully performed dynamic host configuration protocol (DHCP). When the coherency race occurred, the assigned device would not work properly in the guest virtual machine. With this update, the Context coherency is corrected and the race and potentially resulting device assignment failure no longer occurs.

BZ#758028

The align_va_addr kernel parameter was ignored if secondary CPUs were initialized. This happened

because the parameter settings were overridden during the initialization of secondary CPUs. Also, the align_va_addr parameter documentation contained incorrect parameter arguments. With this update, the underlying code has been modified to prevent the overriding and the documentation has been updated. This update also removes the unused code introduced by the patch for BZ#739456.

BZ#758513

Dell systems based on a future Intel processor with graphics acceleration required the selection of the install system with basic video driver installation option. This update removes this requirement.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.119.8. RHSA-2012:0052 — Important: kernel security and bug fix update

Updated kernel packages that fix one security issue and various bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2012-0056, Important

It was found that permissions were not checked properly in the Linux kernel when handling the /proc/[pid]/mem writing functionality. A local, unprivileged user could use this flaw to escalate their privileges. Refer to Red Hat Knowledgebase article 69124 for further information.

Red Hat would like to thank Jüri Aedla for reporting this issue.

Bug Fixes

BZ#768288

The RHSA-2011:1849 kernel update introduced a bug in the Linux kernel scheduler, causing a "WARNING: at kernel/sched.c:5915 thread_return" message and a call trace to be logged. This message was harmless, and was not due to any system malfunctions or adverse behavior. With this update, the WARN_ON_ONCE() call in the scheduler that caused this harmless message has been removed.

BZ#769595

The RHSA-2011:1530 kernel update introduced a regression in the way the Linux kernel maps ELF headers for kernel modules into kernel memory. If a third-party kernel module is compiled on a Red Hat Enterprise Linux system with a kernel prior to RHSA-2011:1530, then loading that module on a system with RHSA-2011:1530 kernel would result in corruption of one byte in the memory reserved for the module. In some cases, this could prevent the module from functioning correctly.

755867

On some SMP systems the tsc may erroneously be marked as unstable during early system boot or while the system is under heavy load. A "Clocksource tsc unstable" message was logged when this occurred. As a result the system would switch to the slower access, but higher precision HPET clock.

The "tsc=reliable" kernel parameter is supposed to avoid this problem by indicating that the system has a known good clock, however, the parameter only affected run time checks. A fix has been put in to avoid the boot time checks so that the TSC remains as the clock for the duration of system runtime.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.119.9. RHSA-2012:0350 — Moderate: kernel security and bug fix update

Updated kernel packages that fix several security issues and bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Security Fixes

CVE-2011-4077, Moderate

A buffer overflow flaw was found in the way the Linux kernel's XFS file system implementation handled links with overly long path names. A local, unprivileged user could use this flaw to cause a denial of service or escalate their privileges by mounting a specially-crafted disk.

CVE-2011-4081, Moderate

Flaws in ghash_update() and ghash_final() could allow a local, unprivileged user to cause a denial of service.

CVE-2011-4132, Moderate

A flaw was found in the Linux kernel's Journaling Block Device (JBD). A local, unprivileged user could use this flaw to crash the system by mounting a specially-crafted ext3 or ext4 disk.

CVE-2011-4347, Moderate

It was found that the kvm_vm_ioctl_assign_device() function in the KVM (Kernel-based Virtual Machine) subsystem of a Linux kernel did not check if the user requesting device assignment was privileged or not. A local, unprivileged user on the host could assign unused PCI devices, or even devices that were in use and whose resources were not properly claimed by the respective drivers, which could result in the host crashing.

CVE-2011-4594, Moderate

Two flaws were found in the way the Linux kernel's __sys_sendmsg() function, when invoked via the sendmmsg() system call, accessed user-space memory. A local, unprivileged user could use these flaws to cause a denial of service.

CVE-2011-4611, Moderate

The RHSA-2011:1530 kernel update introduced an integer overflow flaw in the Linux kernel. On PowerPC systems, a local, unprivileged user could use this flaw to cause a denial of service.

CVE-2011-4622, Moderate

A flaw was found in the way the KVM subsystem of a Linux kernel handled PIT (Programmable Interval Timer) IRQs (interrupt requests) when there was no virtual interrupt controller set up. A local, unprivileged user on the host could force this situation to occur, resulting in the host crashing.

CVE-2012-0038, Moderate

A flaw was found in the way the Linux kernel's XFS file system implementation handled on-disk Access Control Lists (ACLs). A local, unprivileged user could use this flaw to cause a denial of service or escalate their privileges by mounting a specially-crafted disk.

CVE-2012-0045, Moderate

A flaw was found in the way the Linux kernel's KVM hypervisor implementation emulated the syscall instruction for 32-bit guests. An unprivileged guest user could trigger this flaw to crash the guest.

CVE-2012-0207, Moderate

A divide-by-zero flaw was found in the Linux kernel's igmp_heard_query() function. An attacker able to send certain IGMP (Internet Group Management Protocol) packets to a target system could use this flaw to cause a denial of service.

Red Hat would like to thank Nick Bowler for reporting CVE-2011-4081; Sasha Levin for reporting CVE-2011-4347; Tetsuo Handa for reporting CVE-2011-4594; Maynard Johnson for reporting CVE-2011-4611; Wang Xi for reporting CVE-2012-0038; Stephan Bärwolf for reporting CVE-2012-0045; and Simon McVittie for reporting CVE-2012-0207. Upstream acknowledges Mathieu Desnoyers as the original reporter of CVE-2011-4594.

Bug Fixes

BZ#789058

Windows clients never send write requests larger than 64 KB but the default size for write requests in Common Internet File System (CIFS) was set to a much larger value. Consequently, write requests larger than 64 KB caused various problems on certain third-party servers. This update lowers the default size for write requests to prevent this bug. The user can override this value to a larger one to get better performance.

BZ#788003

In certain circumstances, the qla2xxx driver was unable to discover fibre channel (FC) tape devices because the ADISC ELS request failed. This update adds the new module parameter, ql2xasynclogin, to address this issue. When this parameter is set to "0", FC tape devices are discovered properly.

BZ#787580

Socket callbacks use the svc_xprt_enqueue() function to add sockets to the pool->sp_sockets list. In normal operation, a server thread will later take the socket off that list. Previously, on the nfsd daemon shutdown, still-running svc_xprt_enqueue() could re-add an socket to the sp_sockets list just before it was deleted. Consequently, system could terminate unexpectedly by memory corruption in the sunrpc module. With this update, the XPT_BUSY flag is put on every socket and svc_xprt_enqueue() now checks this flag, thus preventing this bug.

BZ#787162

When trying to send a kdump file to a remote system via the tg3 driver, the tg3 NIC (network interface controller) could not establish the connection and the file could not be sent. The kdump kernel leaves

the MSI-X interrupts enabled as set by the crashed kernel, however, the kdump kernel only enables one CPU and this could cause the interrupt delivery to the tg3 driver to fail. With this update, tg3 enables only a single MSI-X interrupt in the kdump kernel to match the overall environment, thus preventing this bug.

BZ#786022

Previously, the cfq_cic_link() function had a race condition. When some processes, which shared ioc issue I/O to the same block device simultaneously, cfq_cic_link() sometimes returned the -EEXIST error code. Consequently, one of the processes started to wait indefinitely. A patch has been provided to address this issue and the cfq_cic_lookup() call is now retried in the described scenario, thus fixing this bug.

BZ#783226

When transmitting a fragmented socket buffer (SKB), the qlge driver fills a descriptor with fragment addresses, after DMA-mapping them. On systems with pages larger than 8 KB and less than eight fragments per SKB, a macro defined the size of the OAL (Outbound Address List) list as 0. For SKBs with more than eight fragments, this would start overwriting the list of addresses already mapped and would make the driver fail to properly unmap the right addresses on architectures with pages larger than 8 KB. With this update, the size of external list for TX address descriptors have been fixed and qlge no longer fails in the described scenario.

BZ#781971

The time-out period in the qla2x00_fw_ready() function was hard-coded to 20 seconds. This period was too short for new QLogic host bus adapters (HBAs) for Fibre Channel over Ethernet (FCoE). Consequently, some logical unit numbers (LUNs) were missing after a reboot. With this update, the time-out period has been set to 60 seconds so that the modprobe utility is able to recheck the driver module, thus fixing this bug.

BZ#772687

Previously, the remove_from_page_cache() function was not exported. Consequently, the module for the Lustre file system did not work correctly. With this update, remove_from_page_cache() is properly exported, thus fixing this bug.

BZ#761536

Due to a regression, the updated vmxnet3 driver used the ndo_set_features() method instead of various methods of the ethtool utility. Consequently, it was not possible to make changes to vmxnet3-based network adapters in Red Hat Enterprise Linux 6.2. This update restores the ability of the driver to properly set features, such as csum or TSO (TCP Segmentation Offload), via ethtool.

BZ#771981

Due to regression, an attempt to open a directory that did not have a cached dentry failed and the EISDIR error code was returned. The same operation succeeded if a cached dentry existed. This update modifies the nfs_atomic_lookup() function to allow fallbacks to normal look-up in the described scenario.

BZ#768916

On a system with an idle network interface card (NIC) controlled by the e1000e driver, when the card transmitted up to four descriptors, which delayed the write-back and nothing else, the run of the watchdog driver about two seconds later forced a check for a transmit hang in the hardware, which found the old entry in the TX ring. Consequently, a false "Detected Hardware Unit Hang" message was issued to the log. With this update, when the hang is detected, the descriptor is flushed and the hang check is run again, which fixes this bug.

BZ#769208

The CFQ (Completely Fair Queuing) scheduler does idling on sequential processes. With changes to the IOeventFD feature, traffic pattern at CFQ changed and CFQ considered everything a thread was doing sequential I/O operations. Consequently, CFQ did not allow preemption across threads in Qemu. This update increases the preemption threshold and the idling is now limited in the described scenario without the loss of throughput.

BZ#771870

A bug in the splice code has caused the file position on the write side of the sendfile() system call to be incorrectly set to the read side file position. This could result in the data being written to an incorrect offset. Now, sendfile() has been modified to correctly use the current file position for the write side file descriptor, thus fixing this bug.

NOTE

Note that in the following common sendfile() scenarios, this bug does not occur: when both read and write file positions are identical and when the file position is not important, for example, if the write side is a socket.

BZ#772884

On large SMP systems, the TSC (Time Stamp Counter) clock frequency could be incorrectly calculated. The discrepancy between the correct value and the incorrect value was within 0.5%. When the system rebooted, this small error would result in the system becoming out of synchronization with an external reference clock (typically a NTP server). With this update, the TSC frequency calculation has been improved and the clock correctly maintains synchronization with external reference clocks.

Users should upgrade to these updated packages, which contain backported patches to correct these issues and fix these bugs. The system must be rebooted for this update to take effect.

4.119.10. RHSA-2012:0481 — Moderate: kernel security, bug fix, and enhancement update

Updated kernel packages that resolve several security issues, fix number of bugs, and add several enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Security Fixes

CVE-2012-0879, Moderate

Numerous reference count leaks were found in the Linux kernel's block layer I/O context handling implementation. This could allow a local, unprivileged user to cause a denial of service.

CVE-2012-1090, Moderate

A flaw was found in the Linux kernel's cifs_lookup() implementation. POSIX open during lookup should only be supported for regular files. When non-regular files (for example, a named (FIFO) pipe or other special files) are opened on lookup, it could cause a denial of service.

CVE-2012-1097, Moderate

It was found that the Linux kernel's register set (regset) common infrastructure implementation did not check if the required get and set handlers were initialized. A local, unprivileged user could use this flaw to cause a denial of service by performing a register set operation with a ptrace() PTRACE_SETREGSET or PTRACE_GETREGSET request.

Red Hat would like to thank H. Peter Anvin for reporting CVE-2012-1097.

Bug Fixes

BZ#805458

Previously, if more than a certain number of qdiscs (Classless Queuing Disciplines) using the autohandle mechanism were allocated a soft lock-up error occurred. This update fixes the maximum loop count and adds the **`cond_resched()`** call in the loop, thus fixing this bug.

BZ#804961

Concurrent look-up operations of the same inode that was not in the per-AG (Allocation Group) inode cache caused a race condition, triggering warning messages to be returned in the **`unlock_new_inode()`** function. Although this bug could only be exposed by NFS or the **`xfsdump`** utility, it could lead to inode corruption, inode list corruption, or other related problems. With this update, the **`XFS_INEW`** flag is set before inserting the inode into the radix tree. Now, any concurrent look-up operation finds the new inode with **`XFS_INEW`** set and the operation is then forced to wait until **`XFS_INEW`** is removed, thus fixing this bug.

BZ#802430

Previously, when isolating pages for migration, the migration started at the start of a zone while the **`free`** scanner started at the end of the zone. Migration avoids entering a new zone by never going beyond what the **`free`** scanner scanned. In very rare cases, nodes overlapped and the migration isolated pages without the LRU lock held, which triggered errors in reclaim or during page freeing. With this update, the **`isolate_migratepages()`** function makes a check to ensure that it never isolates pages from a zone it does not hold the LRU lock for, thus fixing this bug.

BZ#802379

An anomaly in the memory map created by the **`mbind()`** function caused a segmentation fault in Hotspot Java Virtual Machines with the NUMA-aware Parallel Scavenge garbage collector. A backported upstream patch that fixes **`mbind()`** has been provided and the crashes no longer occur in the described scenario.

BZ#786873

Previously, the **`SFQ qdisc`** packet scheduler class had no **`bind_tcf()`** method. Consequently, if a filter was added with the classid parameter to SFQ, a kernel panic occurred due to a null pointer dereference. With this update, the dummy **`.unbind_tcf`** and **`.put`** qdisc class options have been added to conform with the behaviour of other schedulers, thus fixing this bug.

BZ#787764

The kernel code checks for conflicts when an application requests a specific port. If there is no conflict, the request is granted. However, the port auto-selection done by the kernel failed when all ports were bound, even if there was an available port with no conflicts. With this update, the port auto-selection code has been fixed to properly use ports with no conflicts.

BZ#789060

Due to a race condition between the **notify_on_release()** function and task movement between **cpuset** or memory cgroup directories, a system deadlock could occur. With this update, the **cgroup_wq** cgroup has been created and both **async_rebuild_domains()** and **check_for_release()** functions used for task movements use it, thus fixing this bug.

BZ#789061

Previously, the **utime** and **stime** values in the **/proc/<pid>/stat** file of a multi-threaded process could wrongly decrease when one of its threads exited. A backported patch has been provided to maintain monotonicity of **utime** and **stime** in the described scenario, thus fixing this bug.

BZ#801723

The **vmxnet3** driver in Red Hat Enterprise Linux 6.2 introduced a regression. Due to an optimization, in which at least 54 bytes of a frame were copied to a contiguous buffer, shorter frames were dropped as the frame did not have 54 bytes available to copy. With this update, transfer size for a buffer is limited to 54 bytes or the frame size, whichever is smaller, and short frames are no longer dropped in the described scenario.

BZ#789373

In the Common Internet File System (CIFS), the **oplock** break jobs and **async** callback handlers both use the **SLOW-WORK** workqueue, which has a finite pool of threads. Previously, these **oplock** break jobs could end up taking all the running queues waiting for a page lock which blocks the callback required to free this page lock from being completed. This update separates the **oplock** break jobs into a separate workqueue **VERY-SLOW-WORK**, allowing the callbacks to be completed successfully and preventing the deadlock.

BZ#789911

Previously, the **doorbell** register was being unconditionally swapped. If the Blue Frame option was enabled, the register was incorrectly written to the descriptor in the little endian format. Consequently, certain adapters could not communicate over a configured IP address. With this update, the **doorbell** register is not swapped unconditionally, rather, it is always converted to big endian before it is written to the descriptor, thus fixing this bug.

BZ#790007

Previously, due to a bug in a graphics driver in systems running a future Intel processor with graphics acceleration, attempts to suspend the system to the S3/S4 state failed. This update resolves this issue and transitions to the suspend mode now work correctly in the described scenario.

BZ#790338

Prior to this update, the wrong size was being calculated for the **vfinfo** structure. Consequently, networking drivers that created a large number of virtual functions caused warning messages to appear when loading and unloading modules. Backported patches from upstream have been provided to resolve this issue, thus fixing this bug.

BZ#790341

Previously, when a MegaRAID 9265/9285 or 9360/9380 controller got a timeout in the **megaraid_sas** driver, the invalid **SCp.ptr** pointer could be called from the **megasas_reset_timer()** function. As a consequence, a kernel panic could occur. An upstream patch has been provided to address this issue and the pointer is now always set correctly.

BZ#790905

Previously, when pages were being migrated via NFS with an active requests on them, if a particular inode ended up deleted, then the VFS called the **truncate_inode_pages()** function. That function tried to take the page lock, but it was already locked when **migrate_page()** was called. As a consequence, a deadlock occurred in the code. This bug has been fixed and the migration request is now refused if the **PagePrivate** parameter is already set, indicating that the page is already associated with an active read or write request.

BZ#795326

Due to invalid calculations of the **vruntime** variable along with task movement between cgroups, moving tasks between cgroups could cause very long scheduling delays. This update fixes this problem by setting the ***cfs_rq*** and ***curr*** parameters after holding the **rq->lock** lock.

BZ#795335

Due to a race condition, running the **ifenslave -d bond0 eth0** command to remove the slave interface from the bonding device could cause the system to terminate if a networking packet was being received at the same time. With this update, the race condition has been fixed and the system no longer crashes in the described scenario.

BZ#795338

Previously, an unnecessary assertion could trigger depending on the value of the **xpt_pool** field. As a consequence, a node could terminate unexpectedly. The **xpt_pool** field was in fact unnecessary and this update removes it from the **sunrpc** code, thus preventing this bug.

BZ#797241

Due to a race condition, the **mac80211** framework could deauthenticate with an access point (AP) while still scheduling authentication retries with the same AP. If such an authentication attempt timed out, a warning message was returned to kernel log files. With this update, when deauthenticating, pending authentication retry attempts are checked and cancelled if found, thus fixing this bug.

BZ#801718

Prior to this update, the **find_busiest_group()** function used **sched_group->cpu_power** in the denominator of a fraction with a value of **0**. Consequently, a kernel panic occurred. This update prevents the divide by zero in the kernel and the panic no longer occurs.

BZ#798572

When the **nohz=off** kernel parameter was set, kernel could not enter any CPU C-state. With this update, the underlying code has been fixed and transitions to CPU idle states now work as expected.

BZ#797182

Under heavy memory and file system load, the **mapping->nrpages == 0** assertion could occur in the **end_writeback()** function. As a consequence, a kernel panic could occur. This update provides a reliable check for **mapping->nrpages** that prevent the described assertion, thus fixing this bug.

BZ#797205

Due to a bug in the **hid_reset()** function, a deadlock could occur when a Dell iDRAC controller was reset. Consequently, its USB keyboard or mouse device became unresponsive. A patch that fixes the underlying code has been provided to address this bug and the hangs no longer occur in the

described scenario.

BZ#796828

On a system that created and deleted lots of dynamic devices, the 31-bit Linux **ifindex** object failed to fit in the 16-bit **macvtap** minor range, resulting in unusable **macvtap** devices. The problem primarily occurred in a **libvirt**-controlled environment when many virtual machines were started or restarted, and caused **libvirt** to report the following message:

```
Error starting domain: cannot open macvtap tap device /dev/tap222364: No
such device or address
```

With this update, the **macvtap**'s minor device number allocation has been modified so that virtual machines can now be started and restarted as expected in the described scenario.

BZ#799943

The **dm_mirror** module can send discard requests. However, the **dm_io** interface did not support discard requests and running an LVM mirror over a discard-enabled device led to a kernel panic. This update adds support for the discard requests to the **dm_io** interface and kernel panics no longer occur in the described scenario.

BZ#749248

When a process isolation mechanism such as LXC (Linux Containers) was used and the user space was running without the **CAP_SYS_ADMIN** identifier set, a jailed root user could bypass the **dmesg_restrict** protection, creating an inconsistency. Now, writing to **dmesg_restrict** is only allowed when the root has **CAP_SYS_ADMIN** set, thus preventing this bug.

Enhancements

BZ#789371

With this update, the **igb** driver has been updated to the latest upstream version **3.2.10-k** to provide up-to-date hardware support, features and bug fixes.

BZ#800552

This update provides support for the **O_DIRECT** flag for files in FUSE (Filesystem in Userspace). This flag minimizes cache effects of the I/O to and from a file. In general, using this flag degrades performance, but it is useful in special situations, such as when applications do their own caching.

BZ#770651

This update adds support for mount options to restrict access to **/proc/<PID>/** directories. One of the options is called **hidepid=** and its value defines how much information about processes is provided to non-owners. The **gid=** option defines a group that gathers information about all processes. Untrusted users, which are not supposed to monitor tasks in the whole system, should not be added to the group.

Users should upgrade to these updated packages, which contain backported patches to resolve these issues, fix these bugs, and add these enhancements. The system must be rebooted for this update to take effect.

4.119.11. RHSA-2012:0571 — Moderate: kernel security and bug fix update

Updated kernel packages that resolve several security issues and fix a number of bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Security Fixes

CVE-2011-4086, Moderate

A flaw was found in the way the Linux kernel's journal_unmap_buffer() function handled buffer head states. On systems that have an ext4 file system with a journal mounted, a local, unprivileged user could use this flaw to cause a denial of service.

CVE-2012-1601, Moderate

A flaw was found in the way the KVM_CREATE_IRQCHIP ioctl was handled. Calling this ioctl when at least one virtual CPU (VCPU) already existed could lead to a NULL pointer dereference later when the VCPU is scheduled to run. A local, unprivileged user on a KVM host could use this flaw to crash the host.

Bug Fixes

BZ#810454

Previously, the **`eth_type_trans()`** function was called with the **`VLAN`** device type set. If a VLAN device contained a MAC address different from the original device, an incorrect packet type was assigned to the host. Consequently, if the VLAN devices were set up on a bonding interface in Adaptive Load Balancing (ALB) mode, the TCP connection could not be established. With this update, the **`eth_type_trans()`** function is called with the original device, ensuring that the connection is established as expected.

BZ#801329

When short audio periods were configured, the ALSA PCM midlevel code, shared by all sound cards, could cause audio glitches and other problems. This update adds a time check for double acknowledged interrupts and improves stability of the **`snd-aloop`** kernel module, thus fixing this bug.

BZ#802852

Previously, the **`idmapper`** utility pre-allocated space for all user and group names on an NFS client in advance. Consequently, page allocation failure could occur, preventing a proper mount of a directory. With this update, the allocation of the names is done dynamically when needed, the size of the allocation table is now greatly reduced, and the allocation failures no longer occur.

BZ#803881

In a Boot-from-San (BFS) installation via certain iSCSI adapters, driver exported **`sendtarget`** entries in the **`sysfs`** file system but the **`iscsistart`** failed to perform discovery. Consequently, a kernel panic occurred during the first boot sequence. With this update, the driver performs the discovery instead, thus preventing this bug.

BZ#810322

The SCSI layer was not using a large enough buffer to properly read the entire **`BLOCK LIMITS VPD`** page that is advertised by a storage array. Consequently, the ***`WRITE SAME MAX LEN`*** parameter was

read incorrectly and this could result in the block layer issuing discard requests that were too large for the storage array to handle. This update increases the size of the buffer that the **BLOCK LIMITS VPD** page is read into and the discard requests are now issued with proper size, thus fixing this bug.

BZ#805457

A bug in the **try_to_wake_up()** function could cause status change from **TASK_DEAD** to **TASK_RUNNING** in a race condition with an SMI (system management interrupt) or a guest environment of a virtual machine. As a consequence, the exited task was scheduled again and a kernel panic occurred. This update fixes the race condition in the **do_exit()** function and the panic no longer occurs in the described scenario.

BZ#806205

When expired user credentials were used in the **RENEW()** calls, the calls failed. Consequently, all access to the NFS share on the client became unresponsive. With this update, the machine credentials are used with these calls instead, thus preventing this bug most of the time. If no machine credentials are available, user credentials are used as before.

BZ#806859

When the python-perf subpackage was installed, the debug information for the bindings were added to the debuginfo-common subpackage, making it unable to install the debuginfo-common package of a different version. With this update, a separate subpackage is used to store debug information for python-perf, thus fixing this bug.

BZ#809388

Due to the **netdevice** handler for FCoE (Fibre Channel over Ethernet) and the exit path blocking the **keventd** work queue, the **destroy** operation on an NPIV (N_Port ID Virtualization) FCoE port led to a deadlock interdependency and caused the system to become unresponsive. With this update, the **destroy_work** item has been moved to its own work queue and is now executed in the context of the user space process requesting the destroy, thus preventing this bug.

BZ#809372

The **fcoe_transport_destroy** path uses a work queue to destroy the specified FCoE interface. Previously, the **destroy_work** work queue item blocked another single-threaded work queue. Consequently, a deadlock between queues occurred and the system became unresponsive. With this update, **fcoe_transport_destroy** has been modified and is now a synchronous operation, allowing to break the deadlock dependency. As a result, destroy operations are now able to complete properly, thus fixing this bug.

BZ#809378

During tests with active I/O on 256 LUNs (logical unit numbers) over FCoE, a large number SCSI mid layer error messages were returned. As a consequence, the system became unresponsive. This bug has been fixed by limiting the source of the error messages and the hangs no longer occur in the described scenario.

BZ#807158

When running **AF_IUCV** socket programs with IUCV transport, an IUCV **SEVER** call was missing in the callback of a receiving IUCV **SEVER** interrupt. Under certain circumstances, this could prevent z/VM from removing the corresponding IUCV-path completely. This update adds the IUCV **SEVER** call to the callback, thus fixing this bug. In addition, internal socket states have been merged, thus simplifying the **AF_IUCV** code.

BZ#809374

Previously, the AMD IOMMU (input/output memory management unit) driver could use the MSI address range for DMA (direct memory access) addresses. As a consequence, DMA could fail and spurious interrupts would occur if this address range was used. With this update, the MSI address range is reserved to prevent the driver from allocating wrong addresses and DMA is now assured to work as expected in the described scenario.

BZ#811299

Due to incorrect use of the **`list_for_each_entry_safe()`** macro, the enumeration of remote procedure calls (RPCs) priority wait queue tasks stored in the **`tk_wait.links`** list failed. As a consequence, the **`rpc_wake_up()`** and **`rpc_wake_up_status()`** functions failed to wake up all tasks. This caused the system to become unresponsive and could significantly decrease system performance. Now, the **`list_for_each_entry_safe()`** macro is no longer used in **`rpc_wake_up()`**, ensuring reasonable system performance.

BZ#809376

The AMD IOMMU driver used wrong shift direction in the **`alloc_new_range()`** function. Consequently, the system could terminate unexpectedly or become unresponsive. This update fixes the code and crashes and hangs no longer occur in the described scenario.

BZ#809104

Previously, a bonding device had always the UFO (UDP Fragmentation Offload) feature enabled even when no slave interfaces supported UFO. Consequently, the **`tracepath`** command could not return correct path MTU. With this update, UFO is no longer configured for bonding interfaces by default if the underlying hardware does not support it, thus fixing this bug.

BZ#807426

Previously, when the PCI driver switched from MSI/MSI-X (Message Signaled Interrupts) to the INTx emulation while shutting down a device, an unwanted interrupt was generated. Consequently, interrupt handler of IPMI was called repeatedly, causing the system to become unresponsive. This update adds a parameter to avoid using MSI/MSI-X for PCIe native hot plug operations and the hangs no longer occur in the described scenario.

BZ#811135

On NFS, when repeatedly reading a directory, content of which kept changing, the client issued the same **`readdir`** request twice. Consequently, the following warning messages were returned to the **`dmesg`** output:

```
NFS: directory A/B/C contains a readdir loop.
```

This update fixes the bug by turning off the loop detection and letting the NFS client try to recover in the described scenario and the messages are no longer returned.

BZ#806906

The Intelligent Platform Management Interface (IPMI) specification requires a minimum communication timeout of five seconds. Previously, the kernel incorrectly used a timeout of one second. This could result in failures to communicate with Baseboard Management Controllers (BMC) under certain circumstances. With this update, the timeout has been increased to five seconds to prevent such problems.

BZ#804548

Prior to this update, bugs in the **close()** and **send()** functions caused delays and operation of these two functions took too long to complete. This update adds the **IUCV_CLOSED** state change and improves locking for **close()**. Also, the **net_device** handling has been improved in **send()**. As a result, the delays no longer occur.

BZ#804547

When **AF_IUCV** sockets were using the HiperSockets transport, maximum message size for such transports depended on the MTU (maximum transmission unit) size of the HiperSockets device bound to a **AF_IUCV** socket. However, a socket program could not determine maximum size of a message. This update adds the **MSGSIZE** option for the **getsockopt()** function. Through this option, the maximum message size can be read and properly handled by **AF_IUCV**.

BZ#809391

Previously, on a system where intermediate P-states were disabled, the **powernow-k8** driver could cause a kernel panic in the **cpufreq** subsystem. Additionally, not all available P-states were recognized by the driver. This update modifies the drive code so that it now properly recognizes all P-states and does not cause the panics in the described scenario.

Users should upgrade to these updated packages, which contain backported patches to resolve these issues and fix these bugs. The system must be rebooted for this update to take effect.

4.119.12. RHBA-2012:0124 — kernel bug fix update

Updated kernel packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Bug Fix

BZ#781974

An insufficiently designed calculation in the CPU accelerator in the previous kernel caused an arithmetic overflow in the sched_clock() function when system uptime exceeded 208.5 days. This overflow led to a kernel panic on the systems using the Time Stamp Counter (TSC) or Virtual Machine Interface (VMI) clock source. This update corrects the aforementioned calculation so that this arithmetic overflow and kernel panic can no longer occur under these circumstances.

All users are advised to upgrade to these updated packages, which fix this bug. The system must be rebooted for this update to take effect.

4.119.13. RHSA-2012:0743 — Important: kernel security and bug fix update

Updated kernel packages that resolve several security issues and fix a number of bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

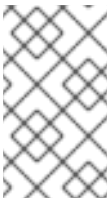
Security Fixes

CVE-2012-0044, Important

A local, unprivileged user could use an integer overflow flaw in **drm_mode_dirtyfb_ioctl()** to cause a denial of service or escalate their privileges.

CVE-2012-2119, Important

A buffer overflow flaw was found in the **macvtap** device driver, used for creating a bridged network between the guest and the host in KVM (Kernel-based Virtual Machine) environments. A privileged guest user in a KVM guest could use this flaw to crash the host.



NOTE

Note that this issue only affected hosts that have the **vhost_net** module loaded with the **experimental_zcopytx** module option enabled (it is not enabled by default), and that also have **macvtap** configured for at least one guest.

CVE-2012-2123, Important

When a set user ID (setuid) application is executed, certain personality flags for controlling the application's behavior are cleared (that is, a privileged application will not be affected by those flags). It was found that those flags were not cleared if the application was made privileged via file system capabilities. A local, unprivileged user could use this flaw to change the behavior of such applications, allowing them to bypass intended restrictions. Note that for default installations, no application shipped by Red Hat for Red Hat Enterprise Linux is made privileged via file system capabilities.

CVE-2012-2136, Important

It was found that the ***data_len*** parameter of the **sock_alloc_send_pskb()** function in the Linux kernel's networking implementation was not validated before use. A privileged guest user in a KVM guest could use this flaw to crash the host or, possibly, escalate their privileges on the host.

CVE-2012-2137, Important

A buffer overflow flaw was found in the **setup_routing_entry()** function in the KVM subsystem of the Linux kernel in the way the Message Signaled Interrupts (MSI) routing entry was handled. A local, unprivileged user could use this flaw to cause a denial of service or, possibly, escalate their privileges.

CVE-2012-1179, Moderate

A race condition was found in the Linux kernel's memory management subsystem in the way **pmd_none_or_clear_bad()**, when called with **mmap_sem** in read mode, and Transparent Huge Pages (THP) page faults interacted. A privileged user in a KVM guest with the ballooning functionality enabled could potentially use this flaw to crash the host. A local, unprivileged user could use this flaw to crash the system.

CVE-2012-2121, Moderate

A flaw was found in the way device memory was handled during guest device removal. Upon successful device removal, memory used by the device was not properly unmapped from the corresponding IOMMU or properly released from the kernel, leading to a memory leak. A malicious user on a KVM host who has the ability to assign a device to a guest could use this flaw to crash the host.

CVE-2012-2372, Moderate

A flaw was found in the Linux kernel's Reliable Datagram Sockets (RDS) protocol implementation. A local, unprivileged user could use this flaw to cause a denial of service.

CVE-2012-2373, Moderate

A race condition was found in the Linux kernel's memory management subsystem in the way **pmd_populate()** and **pte_offset_map_lock()** interacted on 32-bit x86 systems with more than 4GB of RAM. A local, unprivileged user could use this flaw to cause a denial of service.

Red Hat would like to thank Chen Haogang for reporting CVE-2012-0044.

Bug Fixes

BZ#823903

Previously, if creation of an MFN (Machine Frame Number) was lazily deferred, the MFN could appear invalid when is was not. If at this point **read_pmd_atomic()** was called, which then called the paravirtualized **__pmd()** function, and returned zero, the kernel could terminate unexpectedly. With this update, the **__pmd()** call is avoided in the described scenario and the open-coded compound literal is returned instead, thus fixing this bug.

BZ#812953

The **kdump** utility does not support Xen para-virtualized (PV) drivers on Hardware Virtualized Machine (HVM) guests in Red Hat Enterprise Linux 6. Therefore, **kdump** failed to start if the guest had loaded PV drivers. This update modifies underlying code to allow **kdump** to start without PV drivers on HVM guests configured with PV drivers.

BZ#816226

Various problems were discovered in the **iwlwifi** driver happening in the 5 GHz band. Consequently, roaming between access points (AP) on 2.4 GHz and 5 GHz did not work properly. This update adds a new option to the driver that disables the 5 GHz band support.

BZ#816225

The **ctx->vif** identifier is dereferenced in different parts of the **iwlwifi** code. When it was set to **null** before requesting hardware reset, the kernel could terminate unexpectedly. An upstream patch has been provided to address this issue and the crashes no longer occur in the described scenario.

BZ#824429

Previously, with a transparent proxy configured and under high load, the kernel could start to drop packets, return error messages such as **ip_rt_bug: addr1 -> addr2, ?**, and, under rare circumstances, terminate unexpectedly. This update provides patches addressing these issues and the described problems no longer occur.

BZ#819614

Prior to this update, Active State Power Management (ASPM) was not properly disabled, and this interfered with the correct operation of the **hpsa** driver. Certain HP BIOS versions do not report a proper disable bit, and when the kernel fails to read this bit, the kernel defaults to enabling ASPM. Consequently, certain servers equipped with a HP Smart Array controller were unable to boot unless the **pcie_aspm=off** option was specified on the kernel command line. A backported patch has been provided to address this problem, ASPM is now properly disabled, and the system now boots up properly in the described scenario.

BZ#799946

When an adapter was taken down over the RoCE (RDMA over Converged Ethernet) protocol while a workload was running, kernel terminated unexpectedly. A patch has been provided to address this issue and the crash no longer occurs in the described scenario.

BZ#818504

Previously, network drivers that had Large Receive Offload (LRO) enabled by default caused the system to run slow, lose frame, and eventually prevent communication, when using software bridging. With this update, LRO is automatically disabled by the kernel on systems with a bridged configuration, thus preventing this bug.

BZ#818503

Due to a running cursor blink timer, when attempting to hibernate certain types of laptops, the **i915** kernel driver could corrupt memory. Consequently, the kernel could crash unexpectedly. An upstream patch has been provided to make the **i915** kernel driver use the correct console suspend API and the hibernate function now works as expected.

BZ#817466

The slave member of **struct aggregator** does not necessarily point to a slave which is part of the aggregator. It points to the slave structure containing the aggregator structure, while completely different slaves (or no slaves at all) may be part of the aggregator. Due to a regression, the **agg_device_up()** function wrongly used **agg->slave** to find the state of the aggregator. Consequently, wrong active aggregator was reported to the **/proc/net/bonding/bond0** file. With this update, **agg->lag_ports->slave** is used in the described scenario instead, thus fixing this bug.

BZ#816271

As part of mapping the application's memory, a buffer to hold page pointers is allocated and the count of mapped pages is stored in the **do_dio** field. A non-zero **do_dio** marks that direct I/O is in use. However, **do_dio** is only one byte in size. Previously, mapping 256 pages overflowed **do_dio** and caused it to be set to **0**. As a consequence, when large enough number of read or write requests were sent using the **st** driver's direct I/O path, a memory leak could occur in the driver. This update increases the size of **do_dio**, thus preventing this bug.

BZ#810125

Previously, requests for large data blocks with the **ZSECSENDCPRB ioctl()** system call failed due to an invalid parameter. A misleading error code was returned, concealing the real problem. With this update, the parameter for the **ZSECSENDCPRB** request code constant is validated with the correct maximum value. Now, if the parameter length is not valid, the **EINVAL** error code is returned, thus fixing this bug.

BZ#814657

While doing wireless roaming, under stressed conditions, an error could occur in the **ieee80211_mgd_probe_ap_send()** function and cause a kernel panic. With this update, the mac80211 MLME (MAC Layer Management Entity) code has been rewritten, thus fixing this bug.

BZ#816197

Previously, secondary, tertiary, and other IP addresses added to bond interfaces could overwrite the **bond->master_ip** and **vlan_ip** values. Consequently, a wrong IP address could be occasionally used, the MII (Media Independent Interface) status of the backup slave interface went down, and the

bonding master interfaces were switching. This update removes the **master_ip** and **vlan_ip** elements from the bonding and **vlan_entry** structures, respectively. Instead, devices are directly queried for the optimal source IP address for ARP requests, thus fixing this bug.

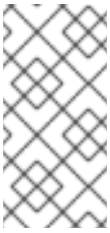
BZ#818505

Red Hat Enterprise Linux 6.1 introduced naming scheme adjustments for emulated SCSI disks used with paravirtual drivers to prevent namespace clashes between emulated IDE and emulated SCSI disks. Both emulated disk types use the paravirt block device **xvd**. Consider the example below:

Table 4.1. The naming scheme example

	Red Hat Enterprise Linux 6.0	Red Hat Enterprise Linux 6.1 or later
emulated IDE	hda -> xvda	unchanged
emulated SCSI	sda -> xvda	sda -> xvde, sdb -> xvdf, ...

This update introduces a new module parameter, **xen_blkfront.sda_is_xvda**, that provides a seamless upgrade path from 6.0 to 6.3 kernel release. The default value of **xen_blkfront.sda_is_xvda** is **0** and it keeps the naming scheme consistent with 6.1 and later releases. When **xen_blkfront.sda_is_xvda** is set to **1**, the naming scheme reverts to the 6.0-compatible mode.



NOTE

Note that when upgrading from 6.0 to 6.3 release, if a virtual machine specifies emulated SCSI devices and utilizes paravirtual drivers and uses explicit disk names such as **xvd[a-d]**, it is advised to add the **xen_blkfront.sda_is_xvda=1** parameter to the kernel command line before performing the upgrade.

BZ#809399

Due to an off-by-one bug in **max_blocks** checks, on the 64-bit PowerPC architecture, the **tmpfs** file system did not respect the **size=** parameter and consequently reported incorrect number of available blocks. A backported upstream patch has been provided to address this issue and **tmpfs** now respects the **size=** parameter as expected.

Users should upgrade to these updated packages, which contain backported patches to resolve these issues and fix these bugs. The system must be rebooted for this update to take effect.

4.119.14. RHBA-2013:1169 — kernel bug fix update

Updated kernel packages that fix several bugs are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The kernel packages contain the Linux kernel, which is the core of any Linux operating system.

Bug Fixes

BZ#977666

A race condition between the read_swap_cache_async() and get_swap_page() functions in the Memory management (mm) code could lead to a deadlock situation. The deadlock could occur only on systems that deployed swap partitions on devices supporting block DISCARD and TRIM operations if kernel preemption was disabled (the !CONFIG_PREEMPT parameter). If the read_swap_cache_async() function was given a SWAP_HAS_CACHE entry that did not have a page in the swap cache yet, a DISCARD operation was performed in the scan_swap_map() function. Consequently, completion of an I/O operation was scheduled on the same CPU's working queue the read_swap_cache_async() was running on. This caused the thread in read_swap_cache_async() to loop indefinitely around its "-EEXIST" case, rendering the system unresponsive. The problem has been fixed by adding an explicit cond_resched() call to read_swap_cache_async(), which allows other tasks to run on the affected CPU, and thus avoiding the deadlock.

BZ#982113

The bnx2x driver could have previously reported an occasional MDC/MDIO timeout error along with the loss of the link connection. This could happen in environments using an older boot code because the MDIO clock was set in the beginning of each boot code sequence instead of per CL45 command. To avoid this problem, the bnx2x driver now sets the MDIO clock per CL45 command. Additionally, the MDIO clock is now implemented per EMAC register instead of per port number, which prevents ports from using different EMAC addresses for different PHY accesses. Also, boot code or Management Firmware (MFW) upgrade is required to prevent the boot code (firmware) from taking over link ownership if the driver's pulse is delayed. The BCM57711 card requires boot code version 6.2.24 or later, and the BCM57712/578xx cards require MFW version 7.4.22 or later.

BZ#982467

If the audit queue is too long, the kernel schedules the kauditd daemon to alleviate the load on the audit queue. Previously, if the current audit process had any pending signals in such a situation, it entered a busy-wait loop for the duration of an audit backlog timeout because the wait_for_auditd() function was called as an interruptible task. This could lead to system lockup in non-preemptive uniprocessor systems. This update fixes the problem by setting wait_for_auditd() as uninterruptible.

BZ#988225

The kernel could rarely terminate instead of creating a dump file when a multi-threaded process using FPU aborted. This happened because the kernel did not wait until all threads became inactive and attempted to dump the FPU state of active threads into memory which triggered a BUG_ON() routine. A patch addressing this problem has been applied and the kernel now waits for the threads to become inactive before dumping their FPU state into memory.

BZ#990080

Due to hardware limits, the be2net adapter cannot handle packets with size greater than 64 KB including the Ethernet header. Therefore, if the be2net adapter received xmit requests exceeding this size, it was unable to process the requests, produced error messages and could become unresponsive. To prevent these problems, GSO (Generic Segmentation Offload) maximum size has been reduced to account for the Ethernet header.

BZ#990085

BE family hardware could falsely indicate an unrecoverable error (UE) on certain platforms and stop further access to be2net-based network interface cards (NICs). A patch has been applied to disable the code that stops further access to hardware for BE family network interface cards (NICs). For a real UE, it is not necessary as the corresponding hardware block is not accessible in this situation.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.119.15. RHSA-2013:0840 — Important: kernel security update

Updated kernel packages that fix one security issue are now available for Red Hat Enterprise Linux 6.2 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2013-2094, Important

This update fixes the following security issue:

* It was found that the Red Hat Enterprise Linux 6.1 kernel update (RHSA-2011:0542) introduced an integer conversion issue in the Linux kernel's Performance Events implementation. This led to a user-supplied index into the perf_swevent_enabled array not being validated properly, resulting in out-of-bounds kernel memory access. A local, unprivileged user could use this flaw to escalate their privileges.

A public exploit that affects Red Hat Enterprise Linux 6 is available.

Refer to Red Hat Knowledge Solution 373743, linked to in the References, for further information and mitigation instructions for users who are unable to immediately apply this update.

Users should upgrade to these updated packages, which contain a backported patch to correct this issue. The system must be rebooted for this update to take effect.

4.119.16. RHBA-2013:1397 — kernel bug fix update

Updated kernel packages that fix two bugs are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The kernel packages contain the Linux kernel, which is the core of any Linux operating system.

Bug Fixes

BZ#1004659

Previously, the be2net driver failed to detect the last port of BE3 (BladeEngine 3) when UMC (Universal Multi-Channel) was enabled. Consequently, two of the ports could not be used by users and error messages were returned. A patch has been provided to fix this bug and be2net driver now detects all ports without returning any error messages.

BZ#1005060

When a copy-on-write fault happened on a Transparent Huge Page (THP), the 2 MB THP caused the cgroup to exceed the "memory.limit_in_bytes" value but the individual 4 KB page was not exceeded. Consequently, the Out of Memory (OOM) killer killed processes outside of a memory cgroup when one or more processes inside that memory cgroup exceeded the "memory.limit_in_bytes" value. With this update, the 2 MB THP is correctly split into 4 KB pages when the "memory.limit_in_bytes" value is exceeded. The OOM kill is delivered within the memory cgroup; tasks outside the memory cgroups are no longer killed by the OOM killer.

Users should upgrade to these updated packages, which contain backported patches to correct these bugs. The system must be rebooted for this update to take effect.

4.119.17. RHSA-2013:1519 — Important: kernel security and bug fix update

Updated kernel packages that fix two security issues and several bugs are now available for Red Hat Enterprise Linux 6.2 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2012-4508, Important

A race condition was found in the way asynchronous I/O and fallocate() interacted when using the ext4 file system. A local, unprivileged user could use this flaw to expose random data from an extent whose data blocks have not yet been written, and thus contain data from a deleted file.

CVE-2013-4299, Moderate

An information leak flaw was found in the way Linux kernel's device mapper subsystem, under certain conditions, interpreted data written to snapshot block devices. An attacker could use this flaw to read data from disk blocks in free space, which are normally inaccessible.

Red Hat would like to thank Theodore Ts'o for reporting CVE-2012-4508, and Fujitsu for reporting CVE-2013-4299. Upstream acknowledges Dmitry Monakhov as the original reporter of CVE-2012-4508.

Bug Fixes

BZ#1017898

When the Audit subsystem was under heavy load, it could loop infinitely in the audit_log_start() function instead of failing over to the error recovery code. This would cause soft lockups in the kernel. With this update, the timeout condition in the audit_log_start() function has been modified to properly fail over when necessary.

BZ#1017902

When handling Memory Type Range Registers (MTRRs), the stop_one_cpu_nowait() function could potentially be executed in parallel with the stop_machine() function, which resulted in a deadlock. The MTRR handling logic now uses the stop_machine() function and makes use of mutual exclusion to avoid the aforementioned deadlock.

BZ#1020519

Power-limit notification interrupts were enabled by default. This could lead to degradation of system performance or even render the system unusable on certain platforms, such as Dell PowerEdge servers. Power-limit notification interrupts have been disabled by default and a new kernel command line parameter "int_pln_enable" has been added to allow users to observe these events using the existing system counters. Power-limit notification messages are also no longer displayed on the console. The affected platforms no longer suffer from degraded system performance due to this problem.

BZ#1021950

Package level thermal and power limit events are not defined as MCE errors for the x86 architecture. However, the mcelog utility erroneously reported these events as MCE errors with the following message:

kernel: [Hardware Error]: Machine check events logged

Package level thermal and power limit events are no longer reported as MCE errors by mcelog. When these events are triggered, they are now reported only in the respective counters in sysfs (specifically, /sys/devices/system/cpu/cpu≶number>/thermal_throttle/).

BZ#1024453

An insufficiently designed calculation in the CPU accelerator could cause an arithmetic overflow in the set_cyc2ns_scale() function if the system uptime exceeded 208 days prior to using kexec to boot into a new kernel. This overflow led to a kernel panic on systems using the Time Stamp Counter (TSC) clock source, primarily systems using Intel Xeon E5 processors that do not reset TSC on soft power cycles. A patch has been applied to modify the calculation so that this arithmetic overflow and kernel panic can no longer occur under these circumstances.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.119.18. RHSA-2013:0882 — Important: kernel security and bug fix update

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 6.2 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-0311, Important

This update fixes the following security issues:

* A flaw was found in the way the vhost kernel module handled descriptors that spanned multiple regions. A privileged guest user in a KVM (Kernel-based Virtual Machine) guest could use this flaw to crash the host or, potentially, escalate their privileges on the host.

CVE-2012-4461, Moderate

A flaw was found in the way the KVM subsystem handled guests attempting to run with the X86_CR4_OSXSAVE CPU feature flag set. On hosts without the XSAVE CPU feature, a local, unprivileged user could use this flaw to crash the host system. (The "grep --color xsave /proc/cpuinfo" command can be used to verify if your system has the XSAVE CPU feature.)

CVE-2012-4542, Moderate

It was found that the default SCSI command filter does not accommodate commands that overlap across device classes. A privileged guest user could potentially use this flaw to write arbitrary data to a LUN that is passed-through as read-only.

CVE-2013-1767, Low

A use-after-free flaw was found in the tmpfs implementation. A local user able to mount and unmount a tmpfs file system could use this flaw to cause a denial of service or, potentially, escalate their privileges.

Red Hat would like to thank Jon Howell for reporting CVE-2012-4461. CVE-2012-4542 was discovered by Paolo Bonzini of Red Hat.

Bug Fixes

BZ#960409

Previously, when open(2) system calls were processed, the GETATTR routine did not check to see if valid attributes were also returned. As a result, the open() call succeeded with invalid attributes instead of failing in such a case. This update adds the missing check, and the open() call succeeds only when valid attributes are returned.

BZ#960418

Previously, the fsync(2) system call incorrectly returned the EIO (Input/Output) error instead of the ENOSPC (No space left on device) error. This was due to incorrect error handling in the page cache. This problem has been fixed and the correct error value is now returned.

BZ#960423

In the RPC code, when a network socket backed up due to high network traffic, a timer was set causing a retransmission, which in turn could cause an even larger amount of network traffic to be generated. To prevent this problem, the RPC code now waits for the socket to empty instead of setting the timer.

BZ#955502

This update fixes a number of bugs in the be2iscsi driver for ServerEngines BladeEngine 2 Open iSCSI devices.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.119.19. RHBA-2013:0584 — kernel bug fix update

Updated kernel packages that fix two bugs are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The kernel packages contain the Linux kernel, which is the core of any Linux operating system.

Bug Fixes

BZ#891862

Previously, NFS mounts failed against Microsoft Windows 8 servers, because the Windows server contained support for the minor version 1 (v4.1) of the NFS version 4 protocol only, along with support for versions 2 and 3. The lack of the minor version 0 (v4.0) support caused Red Hat Enterprise Linux 6 clients to fail instead of rolling back to version 3 as expected. This update fixes this bug and mounting an NFS export works as expected.

BZ#905433

If Time Stamp Counter (TSC) kHz calibration failed, usually on a Red Hat Enterprise Linux 6 virtual machine running inside of QEMU, the init_tsc_clocksource() function divided by zero. This was due to a missing check to verify if the tsc_khz variable is of a non-zero value. Consequently, booting the kernel on such a machine led to a kernel panic. This update adds the missing check to prevent this problem and TSC calibration functions normally.

Users should upgrade to these updated packages, which contain backported patches to fix these bugs. The system must be rebooted for this update to take effect.

4.120. KEXEC-TOOLS

4.120.1. RHSA-2011:1532 — Moderate: kexec-tools security, bug fix, and enhancement update

An updated kexec-tools package that fixes three security issues, various bugs, and adds several enhancements is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. *Common Vulnerability Scoring System* (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

kexec-tools allows a Linux kernel to boot from the context of a running kernel.

Security Fixes

CVE-2011-3588

Kdump used the *Secure Shell* (SSH) **`StrictHostKeyChecking=no`** option when dumping to SSH targets, causing the target kdump server's SSH host key not to be checked. This could make it easier for a man-in-the-middle attacker on the local network to impersonate the **kdump** SSH target server and possibly gain access to sensitive information in the vmcore dumps.

CVE-2011-3589

mkdumprd created initial RAM disk **`(initrd)`** files with world-readable permissions. A local user could possibly use this flaw to gain access to sensitive information, such as the private SSH key used to authenticate to a remote server when **kdump** was configured to dump to an SSH target.

CVE-2011-3590

mkdumprd included unneeded sensitive files (such as all files from the **`/root/.ssh/`** directory and the host's private SSH keys) in the resulting **`initrd`**. This could lead to an information leak when **`initrd`** files were previously created with world-readable permissions.

NOTE

With this update, only the SSH client configuration, known hosts files, and the SSH key configured via the newly introduced sshkey option in **`/etc/kdump.conf`** are included in the **`initrd`**. The default is the key generated when running the **`service kdump propagate`** command, **`/root/.ssh/kdump_id_rsa`**.

Red Hat would like to thank Kevan Carstensen for reporting these issues.

Bug Fixes

BZ#681796

Kdump is a **kexec** based crash dumping mechanism for Linux. *Root System Description Pointer* (RSDP) is a data structure used in the ACPI programming interface. **Kdump** uses **kexec** to boot to a second kernel, the "dump-capture" or "crash kernel", when a dump of the system kernel's memory needs to be taken. On systems using *Extensible Firmware Interface* (EFI), attempting to boot a second kernel using **kdump** failed, the **dump-capture** kernel became unresponsive and the following error message was logged.

```
ACPI Error: A valid RSDP was not found
```

With this update, a new parameter, ***acpi_rsdp***, has been added to the **noefi** kernel command. Now, if EFI is detected, a command is given to the second kernel, in the format, **noefi acpi_rsdp=X**, not to use EFI and simultaneously passes the address of RSDP to the second kernel. The second kernel now boots successfully on EFI machines.

BZ#693025

To reduce the size of the vmcore dump file, **kdump** allows you to specify an external application (that is, a core collector) to compress the data. The core collector was not enabled by default when dumping to a secure location via SSH. Consequently, if users had not specified an argument for **core_collector** in kdump.conf, when **kdump** was configured to dump kernel data to a secure location using SSH, it generated a complete vmcore, without removing free pages. With this update, the default core collector will be **makedumpfile** when **kdump** is configured to use SSH. As a result, the vmcore dump file is now compressed by default.

BZ#707805

Previously, the **mkdumprd** utility failed to parse the **/etc/mdadm.conf** configuration file. As a consequence, **mkdumprd** failed to create an initial RAM disk file system (**initrd**) for **kdump** crash recovery and the **kdump** service failed to start. With this update, **mkdumprd** has been modified so that it now parses the configuration file and builds **initrd** correctly. The **kdump** service now starts as expected.

BZ#708503

In order for Coverity to scan defects in downstream patches separately, it is necessary to make a clean raw build of the source code without patches. However, **kexec-tools** would not build without downstream patches. With this update, by adding a specified patch in **kexec-tools** spec file, **kexec-tools** can now be built from source in the scenario described.

BZ#709441

On 64-bit PowerPC-based systems with more than 1 TB of RAM, the **kexec-tools** utility terminated unexpectedly with a segmentation fault when **kdump** was started, thus preventing crash kernel capture. With this update, the problem has been fixed, **kexec-tools** no longer crashes, and **kdump** can now be used on a system with greater than 1 TB of physical memory.

BZ#719105

The **mkdumprd** utility creates an initial RAM disk file system (**initrd**) for use in conjunction with the booting of a second kernel within the **kdump** framework for crash recovery. Prior to this update, **mkdumprd** became unresponsive when the running kernel was not the same as the target kernel.

With this update the problem has been fixed and **mkdumprd** no longer hangs in the scenario described.

BZ#731236

A regression caused the following erroneous error message to be displayed when **kdump** was setting up Ethernet network connections in order to reach a remote dump target:

```
sed: /etc/cluster_iface: No such file or directory
```

A patch has been applied to correct the problem and the error no longer occurs in the scenario described.

BZ#731394

During **kdump** start up, a check was made to see if the amount of RAM the currently running kernel was using was more than 70% of the amount of RAM reserved for **kdump**. If the memory in use was greater than 70% of the memory reserved, the following error message was displayed.

```
Your running kernel is using more than 70% of the amount of space you
reserved for kdump, you should consider increasing your crashkernel
reservation
```

Due to improvements in conserving memory in the **kexec** kernel the warning is no longer considered valid. This update removes the warning.

BZ#739050

Previously, if **kexec-tools** was installed and **kdump** was not running, installing the fence-agents package caused the following erroneous error message:

```
Non-fatal <unknown> scriptlet failure in rpm package
```

This update corrects the **kexec-tools** spec file and the erroneous error message no longer appears.

BZ#746207

Removing **kexec-tools** on IBM System z resulted in the following error, even though the package was successfully removed.

```
error reading information on service kdump: No such file or directory
```

With this update, changes have been made to the **kexec-tools** spec file and the erroneous error message no longer appears.

BZ#747233

When providing firmware at operating system install time, supplied as part of the Driver Update program (DUP), the installation completed successfully but the operating system would fail on reboot. An error message in the following format was displayed:

```
cp: cannot stat `/lib/firmware/*': No such file or directory
```

With this update, a check for the directory containing the DUP supplied firmware is made and the problem no longer occurs.

Enhancements

BZ#585332

With large memory configurations, some machines take a long time to dump state information when a kernel panic occurs. The cluster software sometimes forced a reboot before the dump completed. With this update, co-ordination between **kdump** and cluster fencing for long kernel panic dumps is added.

BZ#598067

A new configuration option in **kdump.conf**, **force_rebuild**, has been added. When enabled, this option forces the **kdump** init script to rebuild **initrd** every time the system starts, thus ensuring **kdump** has enough storage space on each system start-up.

BZ#725484

On x86, AMD64 & Intel 64 platforms kexec-tools now uses **nr_cpus=1** rather than **maxcpus=1** to save memory required by the second kernel. PowerPC platforms currently cannot handle this feature.

BZ#727892

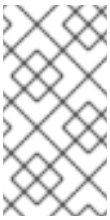
A warning was added to use **maxcpus=1** instead of **nr_cpus=1** for older kernels (see the enhancement above).

BZ#734528

Kdump has been provided with an option so that memory usage can be logged in the second kernel at various stages for debugging memory consumption issues. The second kernel memory usage debugging capability can be enabled via the new **kdump.conf debug_mem_level** option.

BZ#740275, BZ#740277

With this update, **kdump** support for dumping core to **ext4** file systems, and also to **XFS** file systems on data disks (but not the root disk) has been added.

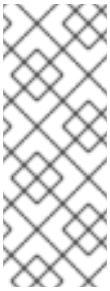


NOTE

> For XFS, the XFS layer product needs to be installed. Layered products are those not included by default in the base Red Hat Enterprise Linux operating system.

BZ#740278

With this update, **kdump** support for dumping core to **Btrfs** file systems has been added.



NOTE

> BusyBox's "findfs" utility does not yet support Btrfs, so UUID/LABEL resolving does not work. Avoid using UUID/LABEL syntax when dumping core to Btrfs file systems. Btrfs itself is still considered experimental; refer to Red Hat Technical Notes.

BZ#748748

Kdump did not check the return code of the **mount** command. Consequently, when the command **mount -t debugfs debug /sys/kernel/debug** was issued in the kdump service script, if the file system was already mounted, the message returned was erroneously logged as an error message. With this update, the logic in the kdump service script has been improved and the kdump service script now functions as expected.

Users of kexec-tools should upgrade to this updated package, which contains backported patches to resolve these issues and add these enhancements.

4.120.2. RHBA-2012:0479 — kexec-tools bug fix update

Updated kexec-tools packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The kexec-tools package contains the /sbin/kexec binary and utilities that together form the user-space component of the kernel's kexec feature. The /sbin/kexec binary facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel.

Bug Fix

BZ#773358

When running kdump after a kernel crash on the system using the ext4 file systems, the kdump initrd could have been created with the zero byte size. This happened because the system waits for several seconds before writing the changes to the disk when using the ext4 file system. Consequently, the kdump initial root file system (rootfs) could not have been mounted and kdump failed. This update modifies kexec-tools to perform the sync operations after creating the initrd. This ensures that initrd is properly written to the disk before trying to mount rootfs so that kdump now successfully proceeds and captures a core dump.

Enhancement

BZ#808466

The kdump utility does not support Xen para-virtualized (PV) drivers on Hardware Virtualized Machine (HVM) guests in Red Hat Enterprise Linux 6. Therefore, kdump failed to start if the guest had loaded PV drivers. This update modifies underlying code to allow kdump to start without PV drivers on HVM guests configured with PV drivers.

All users of kexec-tools are advised to upgrade to these updated packages, which fix this bug add this enhancement.

4.121. KEYUTILS

4.121.1. RHEA-2011:1684 — keyutils bug fix and enhancement update

Updated keyutils packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The keyutils package provides utilities to control the Linux kernel key management facility and to provide a mechanism by which the kernel calls up to user space to get a key instantiated.

Bug Fix

BZ#730002

The keyutils subpackage did not contain a dependency on the keyutils-libs subpackage but rather it contained only an implicit dependency on the libkeyutils.so.[n] shared object files specified as the SONAME variable. As a consequence, the keyutils subpackage could have been updated without applying the newest keyutils libraries, which could have caused keyutils to work incorrectly. To fix this issue, the keyutils spec file has been modified to include an explicit dependency on the version of keyutils-libs that matches the keyutils subpackage. Both subpackages are now updated together.

Enhancement

BZ#727280

Previously, the keyutils subpackages were compiled without the RELRO (read-only relocations) flag. Programs provided by this package and also programs built against the keyutils libraries were thus vulnerable to various attacks based on overwriting the ELF section of a program. To increase the security of keyutils programs and libraries, the keyutils spec file has been modified to use the "-Wl,-z,relro" flags when compiling the packages. As a result, the keyutils subpackages are now provided with partial RELRO protection.

Users are advised to upgrade to these updated keyutils packages, which fix this bug and add this enhancement.

4.122. KRB5

4.122.1. RHSA-2011:1790 — Moderate: krb5 security update

Updated krb5 packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third-party, the Key Distribution Center (KDC).

Security Fix

CVE-2011-1530

A NULL pointer dereference flaw was found in the way the MIT Kerberos KDC processed certain TGS (Ticket-granting Server) requests. A remote, authenticated attacker could use this flaw to crash the KDC via a specially-crafted TGS request.

Red Hat would like to thank the MIT Kerberos project for reporting this issue.

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the krb5kdc daemon will be restarted automatically.

4.122.2. RHBA-2011:1707 — krb5 bug fix update

Updated krb5 packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The Kerberos authentication system allows clients and servers to authenticate to each other using symmetric encryption and the help of a trusted third party, the KDC. This update fixes the following bugs:

BZ#651466

Kerberos version 1.8 and later defaults to disabling support for older encryption types which are no longer believed to be sufficiently strong. When upgrading from older versions of Red Hat Enterprise Linux, a number of services which run at the key distribution center (KDC) need to have their keys reset to include keys for newer encryption types. This update adds a spot-check to the KDC init script which assist in diagnosing this condition.

BZ#701446, BZ#746341

Previously, a client could fail to connect to a KDC if a sufficiently large number of descriptors was already in use. This update modifies the Kerberos libraries to switch to using poll() instead of select(), which does not suffer from this limitation.

BZ#713252, BZ#729068

Previously, the kadmin client could fail to establish a connection with certain older versions of the kadmin daemon. In these situations, the server often logged a diagnostic noting that the client had supplied it with incorrect channel bindings. This update modifies the client to allow it to once again contact those versions of kadmind.

BZ#713518

Previously, a client failed to obtain credentials for authentication from KDCs that rejected requests specifying unrecognized options and that also did not support the canonicalize option. With this update, obtaining credentials also works with these KDCs.

BZ#714217

Previously, locally-applied patches, which attempt to ensure that any files created by the Kerberos libraries are given and keep the correct SELinux file labels, did not correctly ensure that replay cache files kept their labels. This update corrects the patch to cover this case.

BZ#717378

Previously, the Kerberos client libraries could inadvertently trigger an address-to-name lookup inside of the resolver libraries when attempting to derive a principal name from a combination of a service name and a host name, even if the user disabled them using the "rdns" setting in the krb5.conf file. This update modifies the client library to prevent it from triggering these lookups.

BZ#724033

Previously, the kadmind init script could erroneously refuse to start the kadmind server on a KDC, if the realm database was moved to a non-default location, or a non-default kdb backend was in use. This update removes the logic from the init script which caused it to do so.

BZ#729044

Previously, the krb5-debuginfo package excluded several source files used to build the package. This update ensures that the affected files are still included.

BZ#734341

Previously, obtaining the Kerberos credentials for services could fail fail if the target server was in another trusted realm than the client. This update modifies krb5-libs so that the client obtains the credentials as expected.

All Kerberos users are advised to upgrade to these updated packages, which fix these bugs.

4.123. KRB5-APPL

4.123.1. RHSA-2011:1852 — Critical: krb5-appl security update

Updated krb5-appl packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having Critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The krb5-appl packages provide Kerberos-aware telnet, ftp, rcp, rsh, and rlogin clients and servers. Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third-party, the Key Distribution Center (KDC).

Security Fix

CVE-2011-4862

A buffer overflow flaw was found in the MIT krb5 telnet daemon (telnetd). A remote attacker who can access the telnet port of a target machine could use this flaw to execute arbitrary code as root.

Note that the krb5 telnet daemon is not enabled by default in any version of Red Hat Enterprise Linux. In addition, the default firewall rules block remote access to the telnet port. This flaw does not affect the telnet daemon distributed in the telnet-server package.

For users who have installed the krb5-appl-servers package, have enabled the krb5 telnet daemon, and have it accessible remotely, this update should be applied immediately.

All krb5-appl-server users should upgrade to these updated packages, which contain a backported patch to correct this issue.

4.123.2. RHBA-2011:1706 — krb5-appl bug fix and enhancement update

Updated krb5-appl packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The krb5-appl packages contain Kerberos-aware versions of clients and servers for the telnet, FTP, rsh, and rlogin protocols.

Bug Fixes

BZ#713459

Prior to this update, the default PAM configuration for the FTP server incorrectly attempted to use the pam_selinux.so module. As a result, users failed to log in. This update corrects the supplied configuration. Now, the FTP server works as expected.

BZ#713521

Prior to this update, the FTP server did not correctly parse lines in the /etc/ftpusers file which specified user names in combination with the "restrict" keyword. This update modifies the code so that the server parses the "restrict" keyword correctly.

Enhancement

BZ#665834, BZ#736364

Prior to this update, the command-line FTP client in the krb5-appl-clients package did not accept command lines longer than 500 characters. This update removes this limitation.

All users of krb5-appl are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.123.3. RHBA-2012:0550 — krb5-appl bug fix update

Updated krb5-appl packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The krb5-appl packages contain Kerberos-aware versions of telnet, ftp, rsh, and rlogin clients and servers. Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and trusted third-party, the Key Distribution Center (KDC).

Bug Fix

BZ#816689

When executing either the "mdir" or "mls" command, the FTP client stores results returned by the server in a specified local file. Previously, when opening the file, the client did not ensure that the mode value it passed to the fopen() function was properly null-terminated. This could cause unpredictable failures. This update ensures that the value is properly null-terminated so that the failures no longer occur in this scenario.

All users of krb5-appl are advised to upgrade to these updated packages, which fix this bug.

4.124. KSH

4.124.1. RHBA-2012:1428 — ksh bug fix update

An updated ksh package that fixes one bug is now available for Red Hat Enterprise Linux 6 Extended Update Support.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with sh, the original Bourne Shell.

Bug Fix

BZ#863947

Previously, ksh did not allocate the correct amount of memory for its data structures containing information about file descriptors. When running a task that used file descriptors extensively, ksh terminated unexpectedly with a segmentation fault. With this update, the proper amount of memory is allocated and ksh no longer crashes if file descriptors are used extensively.

All users of ksh are advised to upgrade to this updated package, which fixes this bug.

4.124.2. RHBA-2011:1647 — ksh bug fix update

An updated ksh package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with sh, the original Bourne Shell.

Bug Fixes

BZ#702016

Previously, ksh did not always wait for a pipeline to complete when the pipefail option was used. Consequently, a failed exit status was erroneously reported even when the pipeline had not failed. With this update, the code has been improved and the pipefail option now functions as expected.

BZ#702013, BZ#728900

When running a ksh script the exit code of a child process was not preserved. Consequently, when a script asked for such an exit code, the wrong value was reported. With this update, an upstream patch has been applied which fixes the problem.

BZ#702015

File name completion used after an environment variable failed and ksh reported a "bad substitution" error. With this update, an upstream patch has been applied which fixes the problem.

BZ#702011

In POSIX functions, a function defined without using the, "function", keyword, the value of the variable "$0" was changed to the name of the function instead of keeping the original value, the name of the caller function. With this update an upstream patch has been applied to correct the code and ksh keeps the name of the caller function in "$0" as expected.

BZ#701890

Previously, when the ksh built-in "kill" command was called with a very large, non-existent PID value, it was interpreted as " -1". The "-1" argument to the kill command is for terminating all processes. Consequently, all processes owned by the user were killed. With this update a patch has been applied and ksh now checks for a valid process ID.

BZ##683734

If the IFS variable was unset inside a function used in a script, the memory being used was erroneously freed. Consequently, ksh would terminate unexpectedly. With this update, an upstream patch has been applied which still allows the IFS variable to be unset, but no longer frees the memory. Thus the problem is fixed, and ksh no longer crashes in the scenario described.

BZ#702014

Previously, ksh treated an array declaration as a definition. Consequently, the array contained one element after the declaration. This bug has been fixed, and now an array is correctly reported as empty after a declaration.

BZ#742244

Previously, when using ksh, ksh became unresponsive when pipes were used in a "eval" argument. With this update an upstream patch has been applied and the ksh no longer hangs in the scenario described.

BZ#743842

ksh could return the exit code of the previous process to have used the same PID number, when PID numbers were being reused after many hundreds of iterations of a script. With this update the code has been fixed and the error no longer occurs in the scenario described.

All users of ksh are advised to upgrade to this updated package, which fixes these bugs.

4.124.3. RHBA-2012:0004 — ksh bug fix update

An updated ksh package that fixes one bug is now available for Red Hat Enterprise Linux 6.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with sh, the original Bourne Shell.

Bug Fix

BZ#768917

When exiting a subshell after a command substitution, ksh could prematurely exit without any error. With this update, ksh no longer terminates under these circumstances and all subsequent commands are processed correctly.

All users of ksh are advised to upgrade to this updated package, which fixes this bug.

4.125. LESS

4.125.1. RHBA-2011:1575 — less bug fix and enhancement update

An updated less package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The less package contains a text file browser that is similar to the more browser, but with more features ("less is more"). The less text file browser allows users to move backwards in the file as well as forwards. Because the less utility does not need to read the entire input file before it starts, it starts up faster than text editors.

Bug Fixes

BZ#644858

Prior to this update, the online help for the less utility contained incorrect descriptions for several options. With this update, the descriptions have been corrected and the online help describes now all options correctly.

BZ#729025

Prior to this update, a debuginfo file for a binary was missing from the less-debuginfo package. As a result, the crash analysis via the Automatic Bug-Reporting Tool (ABRT) did not work as expected and debugging via GNU Debugger (GDB) could fail. This update modifies the spec file so that the crash analysis via ABRT and debugging via GDB work as expected.

Enhancement

BZ#718498

Prior to this update, the less utility could not view its compressed .xz files.This update adds support for .xz files to lesspipe.sh.

All users of the less text file browser are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.126. LIBARCHIVE

4.126.1. RHBA-2012:0464 — libarchive bug fix update

Updated libarchive packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The libarchive programming library can create and read several different streaming archive formats, including GNU tar and cpio. The library can also read ISO 9660 CD-ROM images.

Bug Fix

BZ#782008

A bug introduced by fixing the CVE-2011-1777 security vulnerability broke functionality of the ISO 9660 CD-ROM image reader and prevented users from opening ISO 9660 images. A patch has been applied to restore full functionality.

All users of libarchive are advised to upgrade to these updated packages, which fix this bug.

4.127. LIBATASMART

4.127.1. RHBA-2012:0703 — libatasmart bug fix update

Updated libatasmart packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The libatasmart packages contain a small and lightweight parser library for ATA S.M.A.R.T. hard disk health monitoring.

Bug Fix

BZ#824918

Due to libatasmart incorrectly calculating the number of bad sectors, certain tools, for example gnome-disk-utility, could erroneously report hard disks with Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T) as failing when logging in GNOME. This update corrects the bad sector calculation, which ensures that tools such as gnome-disk-utility do not report false positive warnings in this scenario.

All users of libatasmart are advised to upgrade to these updated packages, which fix this bug.

4.128. LIBCACARD

4.128.1. RHBA-2011:1518 — libcacard and spice-client bug fix and enhancement update

Updated libcacard and spice-client packages that fix a number of bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol designed for virtual environments. The spice-client package provides the client side of the **SPICE** protocol.

The libcacard package contains the Common Access Card (CAC) emulation library.

BZ#723687

The spice-client package has been upgraded to upstream version 0.8.2, which provides a number of bug fixes and enhancements over the previous version, including:

- Various code cleanup modifications, such as removing unused variables, dead code and typos, have been included.
- Several package build changes, such as enabling a silent build and a cleanup in the configure.ac script have been included.
- White spaces in values for the **`--host-subject`** command line option are now ignored.
- A new **`--version`** command line option for the **`spicec`** command has been added.

BZ#723895

The libcacard package has been upgraded to upstream version 0.15.0, which provides a number of bug fixes and enhancements over the previous version, including a fix for the following bug:

- Some AET middleware did not work correctly with the **`CKM_RSA_X_590`** encrypting mechanism even though it reported support for this mechanism. Consequently, if such middleware was used by libcacard virtual smart cards, smart cards failed to emulate any RSA authentication based operations, such as requesting a security pin or retrieving user certificates. The library has been modified to handle **`CKM_RSA_X590`** failures by falling back to use **`CKM_RSA_PKCS`** encryption. Virtual smart cards now work correctly with AET middleware.

Bug Fixes

BZ#707122

Although old SPICE-related packages (such as cairo-spice) are no longer required to be installed with the spice-client package, they were still needed by a previously installed spice-client or spice-server package. With the **`Obsolete`** lines in the package spec file, updating spice-client forced an update of spice-server as well, and vice versa. With this update, all "Obsolete" lines have been removed from the **`spice-client.spec`** file, and updating spice-client no longer forces the update of spice-server.

BZ#692976

The **`SPICE`** client did not correctly handle monitor setting routines when it was running on a client machine with multiple monitors. As a consequence, the client entered an infinite loop while trying to rearrange monitors, which eventually caused the client to terminate unexpectedly. With this update, the code has been modified to prevent the client from entering this loop, and the client thus no longer crashes.

BZ#725009

The **`SPICE`** client failed to connect to the SPICE server on the target host after a virtual machine had been migrated to a remote machine. This happened when the migration of the virtual machine took longer than the expiration time of the SPICE ticket that was set on the target host. Without a valid password, the SPICE server refused connection from the SPICE client and the SPICE session had to be closed. To prevent this problem, support for spice semi-seamless migration has been added. Other components such as spice-protocol, spice-server and qemu-kvm have also been modified to support this feature. SPICE now allows the SPICE client to connect to the SPICE server on the target host at the very start of the virtual machine migration, just before the migrate monitor command is

given to the **qemu-kvm** application. With a valid ticket on the target host, the SPICE ticket on the destination no longer expires and the SPICE client now remains open when the virtual machine migration is done.

BZ#710461

Due to an incorrect condition in the code, the **SPICE** client could attempt to free memory that has already been freed. Therefore, when the **KDE** desktop screen of the client machine with the running SPICE client was locked, the SPICE client terminated unexpectedly with a segmentation fault after unlocking the screen. The code has been modified to free memory correctly, and the SPICE client no longer crashes in the scenario described.

BZ#692833

When running multiple **SPICE** client sessions at the same time and the screen resolution on the client machine was changed, the SPICE client could often enter an infinite loop in the code. As a consequence, the **X Windows** server consumed up to 100% of CPU and caused the client machine to be unresponsive. With this update, the underlying code has been modified to prevent the client from entering the loop, and the problem no longer occurs.

BZ#712941

The help description for the **`--color-depth`** and **`--disable-effects`** client WAN options was inaccurate. With this update, the **`spicec --help`** command now clearly states that these WAN options have effect only **`if supported by the guest vdagent`**.

BZ#653545

Due to the way the **SPICE** server establishes secured connections, the SPICE client log contained secure-connection messages that included the misleading string, **`connect_unsecure`**. With this update, the function used to establish secure connections has been renamed and secure-connection messages in the client log now contain the **`connect_to_peer`** string.

BZ#732423

On a Linux guest that uses the **Xinerama** extension, **X Windows** creates a non-primary screen surface before it creates the primary screen surface when creating secondary screens on start up. Unfortunately, the **SPICE** client expected an existence of the primary screen surface when it attempted to handle the creation of non-primary screen surfaces. The primary surface did not exist at the time, therefore the SPICE client terminated unexpectedly. With this update, the SPICE client now ensures that the screen exists before starting operations on it. The SPICE client no longer crashes in the scenario described.

BZ#723567

Previously, the **`--smartcard-db`** client command line option was not handled properly. As a consequence, when running with this option, the **SPICE** client terminated with the following error message:

```
Error: unhandled exception: cmd line error
```

With this update, the **`--smartcard-db`** option is now handled properly and the SPICE client works as expected using this option.

BZ#712938

When attempting to connect to a Linux guest using the **SPICE** client with WAN options and the

SPICE agent (**vdagent**) was running on the guest, the client initiated handshaking. If the vdagent did not support WAN options, it did not reply to the client and connection thus failed with the **vdagent** timeout. Also with certain WAN options, such as **--color-depth 16**, the attempt to connect failed with the vdagent timeout even though no **vdagent** was running on the guest. With this update, the SPICE client checks capabilities of the vdagent. If vdagent does not support WAN options or there is no **vdagent** running on the guest, the client continues with the message sequence initiation and connection is now successful.

BZ#696964

Due to a missing error code setting in the source code, the **SPICE** client returned **exit code 0** when running without the **--host** command line option, although the client correctly displayed the following error message:

```
spicec: missing --host
```

With this update, the missing line in the code has been added, and the SPICE client now correctly exits with the **error code 14** in this scenario.

All users of libcacard and spice-client are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.129. LIBCAP

4.129.1. RHSA-2011:1694 — Low: libcap security and bug fix update

Updated libcap packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libcap packages provide a library and tools for getting and setting POSIX capabilities.

Security Fix

CVE-2011-4099

It was found that capsh did not change into the new root when using the "--chroot" option. An application started via the "capsh --chroot" command could use this flaw to escape the chroot restrictions.

Bug Fix

BZ#730957

Previously, the libcap packages did not contain the capsh(1) manual page. With this update, the capsh(1) manual page is included.

All libcap users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.130. LIBCGROUP

4.130.1. RHBA-2011:1225 — libcgroup bug fix update

An updated libcgroup package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The libcgroup package provides tools and libraries to control and monitor control groups.

Bug Fix

BZ#715413

Prior to this update, when installing the libcgroup package, a new group "cgred" was erroneously created as a user group (starting with GID 500) and not as a system group (with GID lower than 500). As a result, newly created users could have had UID different to GID. With this update, the "cgred" group is now created correctly as the system group with GID lower than 500. This update does not change GID of the "cgred" group if the group already exists on the system.

All users are advised to upgrade to this updated libcgroup package, which fixes this bug.

4.131. LIBCMPIUTIL

4.131.1. RHEA-2011:1586 — libcmpiutil enhancement update

An updated libcmpiutil package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The libcmpiutil library provides an application programming interface (API) for performing common tasks with various Common Manageability Programming Interface (CMPI) providers.

Enhancement

BZ#694550

With this update, the performance and the interface of the libcmpiutil library have been enhanced, which is used by the libvirt-cim package.

All libcmpiutil users are advised to upgrade to this updated package, which adds this enhancement.

4.132. LIBESMTP

4.132.1. RHEA-2011:1775 — libesmtp enhancement update

An updated libesmtp package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

LibESMTP is a library to manage posting or submitting electronic mail using SMTP to a preconfigured Mail Transport Agent (MTA). The libesmtp package is required by Open MPI.

Enhancement

BZ#738760

Previously, LibESMTP was not shipped with Red Hat Enterprise Linux 6 on the 64-bit PowerPC platform. This update adds the LibESMTP package to the 64-bit PowerPC variant, as a requirement of the updated OpenMPI. Note, that this update does not contain any changes for other architectures.

All users requiring libesmtp on the 64-bit PowerPC architecture are advised to install this package, which adds this enhancement.

4.133. LIBGCRYPT

4.133.1. RHEA-2011:1734 — libgcrypt enhancement update

An updated libgcrypt package that add an enhancement is now available for Red Hat Enterprise Linux 6.

The libgcrypt package contains a library which provides general-purpose implementations of various cryptographic algorithms.

Enhancement

BZ#727283

With this update, the libgcrypt library has been recompiled with read-only relocation support that improves the security vulnerability properties of applications that use the library.

All users of libgcrypt are advised to upgrade to this updated package, which adds this enhancement.

4.133.2. RHEA-2012:0486 — libgcrypt enhancement update

Updated libgcrypt packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.

Enhancement

BZ#810320

With Federal Information Processing Standards (FIPS) mode enabled, the libgcrypt library always started in the soft FIPS mode which allows applications to use the MD5 cryptographic hash algorithm. The libgcrypt API previously did not allow the library to programmatically switch from the soft FIPS mode to the enforced FIPS mode. With this update, if the application does not need MD5 support for the Transport Layer Security (TLS) protocol or non-cryptographic purposes, libgcrypt can be preset in the enforced FIPS mode.

All users of libgcrypt are advised to upgrade to these updated packages, which add this enhancement.

4.134. LIBGPG-ERROR

4.134.1. RHBA-2011:1717 — libgpg-error enhancement update

An updated libgpg-error package is now available for Red Hat Enterprise Linux 6.

The libgpg-error library provides a set of common error codes and definitions which are shared by the gnupg, libgcrypt and other packages.

Enhancement

BZ#727287

Previously, the libgpg-error package was compiled without the RELRO (read-only relocations) flag. Programs provided by this package were thus vulnerable to various attacks based on overwriting the ELF section of a program. To increase the security of the libgpg-error library, the libgpg-error spec file has been modified to use the "-Wl,-z,relro" flags when compiling the package. As a result, the libgpg-error package is now provided with partial RELRO protection.

Users of libgpg-error are advised to upgrade to this updated package, which adds this enhancement.

4.135. LIBGUESTFS

4.135.1. RHBA-2011:1512 — libguestfs bug fix and enhancement update

Updated libguestfs packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The libguestfs packages contain a library, which is used for accessing and modifying guest disk images.

Bug Fixes

BZ#603000

Previously, the **`do_part_get_bootable()`** API function parsed the output of parted with an assumption that the partition layout on the guest image was well ordered. As a consequence, the **part-get-bootable** API would produce an incorrect result or even terminate with disks where the partitions were not in the usual order or were missing. With this update, the source code is modified so that **libuguestfs** can correctly handle disks with unordered partitions.

BZ#627835

Previously, **`libguestfs`** protocol lost synchronization when using the **`upload`** command in the **`guestfish`** command line tool before mounting any disks. Uploading files failed and an error message was reported due to the library and the daemon sending cancel messages in an incorrect order. With this update, if the daemon detects cancellation, it sends the remaining data in its output buffer instead of discarding it.

BZ#666578, BZ#678231

Previously, if guests used the LABEL or UUID (Universal Unique Identifier) identifiers for swap devices in the guest **`/etc/fstab`** file, the **virt-inspector** utility reported the **`unknown filesystem`** error message. The source code has been modified, and the utility now works correctly and no longer displays error messages.

BZ#682980

Prior to this update, libguestfs could have incorrectly detected Red Hat Enterprise Linux Desktop distributions as a "redhat-based" instead of "redhat". As a consequence, the **virt-v2v** utility failed to convert such guests. With this update, libguestfs is modified to detect these distributions correctly as "redhat". Now, conversion is successful.

BZ#684980

Calling the **`guestfs_kill_subprocess()`** function and then closing the connection handle by calling **`guestfs_close()`** could cause the libguestfs connection to become unresponsive. The

source code has been modified to close the connection correctly so that the connections no longer hangs.

BZ#685009

After the resize operation, the **ntfsresize** utility marks the file system as requiring a consistency check. As a consequence, an error message can appear when resizing the same file system multiple times in a row without rebooting the virtual machine. With this update, the ntfsresize(8) manual page describes this behavior.

BZ#688062

Previously, when pressing the tab key in the **guestfish** command line tool, the mapped devices created by **luks-open** were not listed. With this update, /dev/mapper/ paths are added to tab-completion and the devices are displayed when pressing the tab key.

BZ#690358

Querying a fully-virtualized guest works reliably only for Linux guests. With this update, the virt-inspector(1) manual page is modified to note this.

BZ#692394

Previously, the **inspect-list-applications** API and **virt-inspector2** utility did not detect 32-bit applications installed under the WoW64 (Windows 32-bit on Windows 64-bit) emulator on a 64-bit Windows guest. With this update, the source code is modified to display the installed applications with their description in the output.

BZ#693306

Iterables passed instead of plain lists could cause the RuntimeError exception to be thrown when calling libguestfs' Python interface. The Python bindings have been modified so that any iterable argument can be used as a list.

BZ#695881

Previously, the **virt-make-fs** tool generated the **qemu-img** command which contained an incorrect decimal point in the output. As a result, an error message was reported. With this update, the source code is modified so that the **virt-make-fs** tool invokes **qemu-img** correctly in all cases.

BZ#713529

Due to incorrect mounting of guest file systems, the **virt-v2v** utility could fail when the guest **/etc/fstab** file contained file systems marked with LABEL. This update modifies the source code so that the file systems are mounted correctly. As a result, **virt-v2v** no longer fails.

BZ#725563

With this update, libguestfs is rebuilt against the latest parted package, which adds support for the ***Legacy BIOS Bootable*** flag in the **GPT** (GUID Partition Table) attribute field.

BZ#727178

Prior to this update, a build error prevented libguestfs from working on **LUKS** (Linux Unified Key Setup) encrypted disks. As a result, loading of shared libraries failed with an error message. An upstream patch has been applied to address this issue and libguestfs now works correctly on LUKS devices.

BZ#729887

This update adds the description of typecheck lenses in the guestfish(1) manual page.

BZ#730248

The guestfish(1) manual page has been modified to mention that **`guestfish --remote run`** should not be used in a command substitution context.

Enhancement

BZ#672491

Prior to this update, the **`guestfs_last_errno()`** function was not exposed in the Perl bindings. As a consequence, it was not directly possible to determine the precise cause of some failures. To fix this problem, guestfs_last_errno() is now exposed in the Perl bindings.

All users of libguestfs are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.135.2. RHEA-2012:0458 — libguestfs enhancement update

Enhanced libguestfs packages are now available for Red Hat Enterprise Linux 6.

[Updated 6 Apr 2011] The text of this advisory has been updated to reflect the fact that these packages are not new in Red Hat Enterprise Linux 6.

The libguestfs library allows guest disk images to be accessed and modified. It also enables the making of batch configuration changes to guests, manages migrations between virtualization systems (but also see the virt-p2v utility), obtains information about disk usage (see also the virt-df utility), performs partial backups, guest clones and partial guest clones, and is able to carry out configuration changes to the registry, UUI, and hostname, among other duties.

The libguestfs library can be linked with C and C++ management programs.

The guestfish package enables shell scripting and command line access to libguestfs.

The libguestfs-mount package allows guest file systems to be mounted on the host using the FUSE (Filesystem in Userspace) file system.

Included among these packages are several which enable language bindings:

- for Perl bindings, see the perl-Sys-Guestfs package.
- for OCaml bindings, see the ocaml-libguestfs-devel package.
- for Python bindings, see the python-libguestfs package.
- for Ruby bindings, see the ruby-libguestfs package.
- for Java bindings, see the libguestfs-java-devel package.

Enhancement

BZ#810251

This enhancement update moves the python-libguestfs package from the Red Hat Enterprise Linux 6 Optional channels to the Red Hat Enterprise Linux 6 base channels. This update does not make any other changes to these packages.

All users who require libguestfs should install these enhanced packages.

4.136. LIBHBAAPI

4.136.1. RHBA-2011:1605 — libhbaapi bug fix and enhancement update

An updated libhbaapi package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The Host Bus Adapter API is a C-level project to manage Fibre Channel Host Bus Adapters.

The package has been upgraded to upstream version 2.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#719585)

Users are advised to upgrade to this updated libhbaapi package, which fixes these bugs and adds these enhancements.

4.137. LIBHBALINUX

4.137.1. RHBA-2011:1606 — libhbalinux bug fix and enhancement update

An updated libhbalinux package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The libhbalinux package contains the Host Bus Adapter API (HBAAPI) vendor library which uses standard kernel interfaces to obtain information about Fiber Channel Host Buses (FC HBA) in the system.

The package has been upgraded to upstream version 1.0.12, which provides a number of bug fixes and enhancements over the previous version. (BZ#719584)

Users are advised to upgrade to this updated libhbalinux package, which fixes these bugs and adds these enhancements.

4.138. LIBHUGETLBFS

4.138.1. RHEA-2011:1685 — libhugetlbfs bug fix and enhancement update

Updated libhugetlbfs packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The libhugetlbfs packages provide the library and utilities that are used to interact with the Linux hugetlbfs file system to make large pages available to applications in a transparent manner.

The libhugetlbfs packages have been upgraded to upstream version 2.12, which provide a number of bug fixes and add additional administrator support for using large pages over the previous version. The libhugetlbfs library and utilities now increase overall system performance, especially for large memory systems. The packages are synchronized with kernel support. (BZ#630171)

All users of libhugetlbfs are advised to upgrade to these updated packages which fix these bugs and add this enhancement.

4.139. LIBICA

4.139.1. RHBA-2011:1567 — libica bug fix and enhancement update

Updated libica packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libica library contains a set of functions and utilities for accessing the IBM eServer Cryptographic Accelerator (ICA) hardware on the IBM System z.

The libica library has been upgraded to version 2.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#694247)

All libica users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.140. LIBNIH

4.140.1. RHEA-2011:1672 — libnih enhancement update

An updated libnih package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The libnih package includes a small library for C application development. The library is similar to other C libraries, such as glib.

Enhancement

BZ#727284

Previously, the libnih package was compiled without the read-only relocations (RELRO) flag. Programs built against the libnih library could be vulnerable to various attacks based on overwriting the ELF section of a program. To enhance the security, the libnih package is now provided with partial RELRO support.

All users of libnih are advised to upgrade to this updated package, which adds this enhancement.

4.141. LIBPNG

4.141.1. RHSA-2012:0317 — Important: libpng security update

Updated libpng and libpng10 packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Security Fix

CVE-2011-3026

A heap-based buffer overflow flaw was found in libpng. An attacker could create a specially-crafted PNG image that, when opened, could cause an application using libpng to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of libpng and libpng10 should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libpng or libpng10 must be restarted for the update to take effect.

4.141.2. RHSA-2012:0407 — Moderate: libpng security update

Updated libpng packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Security Fix

CVE-2011-3045

A heap-based buffer overflow flaw was found in the way libpng processed compressed chunks in PNG image files. An attacker could create a specially-crafted PNG image file that, when opened, could cause an application using libpng to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of libpng should upgrade to these updated packages, which correct this issue. For Red Hat Enterprise Linux 5, they contain a backported patch. For Red Hat Enterprise Linux 6, they upgrade libpng to version 1.2.48. All running applications using libpng must be restarted for the update to take effect.

4.141.3. RHSA-2012:0523 — Moderate: libpng security update

Updated libpng packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Security Fix

CVE-2011-3048

A heap-based buffer overflow flaw was found in the way libpng processed tEXt chunks in PNG image files. An attacker could create a specially-crafted PNG image file that, when opened, could cause an application using libpng to crash or, possibly, execute arbitrary code with the privileges of the user

running the application.

Users of libpng should upgrade to these updated packages, which correct this issue. For Red Hat Enterprise Linux 5, they contain a backported patch. For Red Hat Enterprise Linux 6, they upgrade libpng to version 1.2.49. All running applications using libpng must be restarted for the update to take effect.

4.142. LIBSELINUX

4.142.1. RHBA-2011:1559 — libselinux bug fix update

Updated libselinux packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The libselinux packages contain the core library of an SELinux system. The libselinux library provides an API for SELinux applications to get and set process and file security contexts, and to obtain security policy decisions. It is required for any applications that use the SELinux API, and used by all applications that are SELinux-aware.

Bug Fixes

BZ#698583

Prior to this update, Python bindings for the restorecon command required a user to specify the entire path. Consequent to this, an attempt to use the selinux.restorecon() function with a relative path failed with the following error message:

```
OSError: [Errno 2] No such file or directory
```

This update corrects the Python bindings to allow the use of the selinux.restorecon() function with a relative path or just a file name.

BZ#706049

Previously, the is_selinux_enabled() function may have incorrectly returned a positive value even when the machine was disabled. This happened when the same process that made the calls to disable SELinux attempted to determine if SELinux is enabled, because the selinux_mnt variable was not properly freed and still contained old data. With this update, a patch has been applied to make sure the selinux_mnt variable is now properly freed, and the is_selinux_enabled() function works as expected.

BZ#748471

When a semanage login record was set up using a group name and the number of elements in the group was too large, login programs failed to log in the user with the correct context. This update corrects the libselinux library to return all users within a group so that the correct SELinux user record is used. As a result, users with the correct context can now log in as expected in this scenario.

All users of libselinux are advised to upgrade to these updated packages, which fix these bugs.

4.142.2. RHEA-2012:0460 — libselinux enhancement update

Enhanced libselinux packages are now available for Red Hat Enterprise Linux 6.

[Updated 6 Apr 2011] The text of this advisory has been updated to reflect the fact that these packages are not new in Red Hat Enterprise Linux 6.

Security-enhanced Linux (SELinux) is a feature of the Linux kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement, Role-based Access Control, and Multi-level Security. The libselinux library provides an API for SELinux applications to get and set process and file security contexts and to obtain security policy decisions, and is required for any applications that use the SELinux API.

This enhancement update moves the selinux-ruby package from the Red Hat Enterprise Linux 6 Optional channels to the Red Hat Enterprise Linux 6 base channels. This update does not make any other changes to these packages. (BZ#810119)

All users who require SELinux should install these enhanced packages.

4.142.3. RHEA-2013:0809 — libselinux enhancement update

Updated libselinux packages that add one enhancement are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The libselinux packages contain the core library of an SELinux system. The libselinux library provides an API for SELinux applications to get and set process and file security contexts, and to obtain security policy decisions. It is required for any applications that use the SELinux API, and used by all applications that are SELinux-aware.

Enhancement

BZ#956981

Previously, a substitution of the "/" directory was not directly possible. With this update, support for a substitution of the root directory has been added to allow proper labeling of all directories and files under an alternative root directory.

Users of libselinux are advised to upgrade to these updated packages, which adds this enhancement.

4.143. LIBSEMANAGE

4.143.1. RHBA-2011:1770 — libsemanage bug fix update

Updated libsemanage packages that fix file creation when umask is changed.

The libsemanage library provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, as well as by programs such as load_policy, which must perform specific transformations on binary policies (for example, customizing policy boolean settings).

Bug Fix

BZ#747345

When running semanage commands while umask is set to 027 (or to a similar value that restricts a non-priviledged user from reading files created with such a file-creating mask), semanage changed the permissions of certain files such as the /etc/selinux/mls/contexts/files/file_contexts file. As a consequence, non-priviledged processes were not able to read such files and certain commands such as the restorecon command failed to run on these files. To solve this problem, libsemanage has

been modified to save and clear umask before libsemanage creates context files and then restore it after the files are created so the file permissions are readable by non-priviledged processes. Operations on these context files now work as expected.

All users of libsemange are advised to upgrade to these updated packages, which fix this bug.

4.144. LIBSEPOL

4.144.1. RHBA-2011:1689 — libsepol enhancement update

Enhanced libsepol packages are now available for Red Hat Enterprise Linux 6.

The libsepol library provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, as well as by programs like load_policy that need to perform specific transformations on binary policies (for example, customizing policy boolean settings).

Enhancement

BZ#727285

Previously, the libsepol packages were compiled without the RELRO (read-only relocations) flag. As a consequence, programs provided by this package and also programs built against the libsepol libraries were vulnerable to various attacks based on overwriting the ELF section of a program. To increase the security of libsepol programs and libraries, the libsepol spec file has been modified to use the "-Wl,-z,relro" flags when compiling the packages. As a result, the libsepol packages are now provided with partial RELRO protection.

Users of libsepol are advised to upgrade to these updated packages, which add this enhancement.

4.145. LIBSNDFILE

4.145.1. RHBA-2011:1226 — libsndfile bug fix update

An updated libsndfile package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The libsndfile package provides a library for reading and writing sound files.

Bug Fix

BZ#664323

Prior to this update, the libsndfile package was built without the Ogg container format support. As a result, applications using the libsndfile library were not able to work with the Ogg format. With this update, the problem has been fixed so that applications can now work with the Ogg format as expected.

All users of libsndfile are advised to upgrade to this updated package, which fixes this bug.

4.146. LIBSSH2

4.146.1. RHBA-2012:0431 — libssh2 bug fix update

An updated libssh2 package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The libssh2 package provides a library that implements the SSH2 protocol.

Bug Fixes

BZ#803389

Previously, an insufficient data type was used for certain bit shift operations in the libssh2 code. This could result in an arithmetic overflow, which caused the curl utility to terminate unexpectedly when downloading files larger than 2 GB over the SFTP protocol. With this update, the underlying code has been modified to use the correct data type and curl now works as expected in the scenario described.

BZ#805026

When sending a large amount of data over SSH, libssh2 could, under certain circumstances, fail to resume an interrupted key exchange. Instead of that, further data was erroneously sent, which caused the remote site to close the connection immediately. This update modifies the code of libssh2 so that libssh2 now properly resumes the interrupted key exchange before sending any further data. The connection remains open and the data transfer proceeds as expected.

All users of libssh2 are advised to upgrade to this updated package, which fixes these bugs. After installing this updated package, all running applications using libssh2 have to be restarted for this update to take effect.

4.147. LIBTASN1

4.147.1. RHSA-2012:0427 — Important: libtasn1 security update

Updated libtasn1 packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

libtasn1 is a library developed for ASN.1 (Abstract Syntax Notation One) structures management that includes DER (Distinguished Encoding Rules) encoding and decoding.

Security Fix

CVE-2012-1569

A flaw was found in the way libtasn1 decoded DER data. An attacker could create carefully-crafted DER encoded input (such as an X.509 certificate) that, when parsed by an application that uses libtasn1 (such as applications using GnuTLS), could cause the application to crash.

Red Hat would like to thank Matthew Hall of Mu Dynamics for reporting this issue.

Users of libtasn1 are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. For the update to take effect, all applications linked to the libtasn1 library must be restarted, or the system rebooted.

4.148. LIBTIFF

4.148.1. RHSA-2012:0468 — Important: libtiff security update

Updated libtiff packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

Security Fix

CVE-2012-1173

Two integer overflow flaws, leading to heap-based buffer overflows, were found in the way libtiff attempted to allocate space for a tile in a TIFF image file. An attacker could use these flaws to create a specially-crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code.

All libtiff users should upgrade to these updated packages, which contain a backported patch to resolve these issues. All running applications linked against libtiff must be restarted for this update to take effect.

4.149. LIBTIRPC

4.149.1. RHBA-2011:1745 — libtirpc bug fix update

An updated libtirpc package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The libtirpc package contains SunLib's implementation of transport independent RPC (TI-RPC) documentation. This includes a library required by programs in the nfs-utils and rpcbind packages.

Bug Fix

BZ#714015

Due to certain errors and missing code in libtirpc, user space NFS servers were not able to fully utilize the RPCSEC_GSS security protocol, which allows remote procedure call (RPC) protocols to access the Generic Security Services Application Programming Interface (GSS-API). With this update, the problems have been fixed in the libtirpc code. The RPCSEC_GSS protocol now can be used by NFS servers properly.

All users of libtirpc are advised to upgrade to this updated package, which fixes this bug.

4.150. LIBVIRT

4.150.1. RHBA-2011:1513 — libvirt bug fix and enhancement update

Updated libvirt packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems.

Bug Fixes

BZ#710150

Due to a bug in the qemuAuditDisk() function, hot unplug failures were never audited, and a hot unplug success was audited as a failure. This bug has been fixed, and auditing of disk hot unplug operations now works as expected.

BZ#711151

Previously, a bug in the qemu-img command line arguments prevented the creation of encrypted volumes. This update fixes the bug, and encrypted volumes can now be successfully created.

BZ#711206

Previously, when a debug process was being activated, the act of preparing a debug message ended up with dereferencing a Universally Unique Identifier (UUID) prior to the NULL argument check. As a consequence, an API running the debug process sometimes terminated unexpectedly with a segmentation fault. With this update, a patch has been applied to address this issue, and crashes no longer occur in the described scenario.

BZ#742646

Due to a programming mistake in the initialization code of the libvirtd daemon, the QEMU driver could have failed to find the user or group ID of the qemu application on the system. As a consequence, libvirtd failed to start. With this update, the error has been corrected and libvirtd now starts as expected.

BZ#741217

If the QEMU driver failed to update information about currently allocated memory, installing a new virtual machine failed with the following error message:

```
ERROR    cannot send monitor command '{"execute":"query-balloon"}':
Connection reset by peer
```

With this update, the driver has been modified to not consider this behavior as fatal. Installation now proceeds and finishes as expected.

BZ#690695

Previously, when running the "virsh vol-create-from" command on a Logical Volume Manager (LVM) storage pool, performance of the command was very low and the operation consumed an excessive amount of time. This bug has been fixed in the virStorageVolCreateXMLFrom() function, and the performance problem of the command no longer occurs.

BZ#690175

When migrating a QEMU domain and restarting the libvirtd daemon, the migration was not properly canceled. The domain was left on the target host or ended up in an unexpected state on the source host. With this update, the libvirtd daemon tracks ongoing migrations in a persistent file, and properly cancels them when the daemon is being restarted.

BZ#738146

The "virsh dump" command can fail to dump the core of a domain if the user sets incorrect permissions for the destination directory. Previously, the virsh(1) man page did not provide any information about the permissions required to successfully complete a domain core dump. This information is now included in the man page.

BZ#734773

When shutting down a guest operating system, libvirt killed the QEMU process without giving it enough time to flush all disk I/O buffers. This led in certain cases to loss of data or corruption of the virtual disk. With this update, libvirt gives QEMU enough time to flush the buffers and exits instead of forcibly killing the process.

BZ#738148

When the user started a virtual machine, changed its definition, and migrated the virtual machine, the new settings were not available on the destination. With this update, the settings are transferred to the destination by a live XML file which includes current settings of the running virtual machine. Now, settings are kept during the migration.

BZ#669549

Previously, libvirt did not exercise enough control over whether a domain change should affect the running domain, the persistent configuration, or both. Various virsh commands were inconsistent, and attempts to change a configuration of a running domain did not persist to the next boot. With this update, several libvirt commands have new flags to distinguish between live and persistent configurations. The corresponding virsh commands can be used with the "--config" and "--live" flags to provide a more consistent interface. Management applications have finer control over whether various configuration changes affect hot plug, next boot, or both.

BZ#674537

Various logic bugs affected the handling of snapshots in libvirt. Among these, restarting the libvirtd daemon would lose track of the current snapshot, and a change in QEMU behavior would trigger a latent bug in libvirt's ability to restore certain snapshots. Snapshots were therefore unreliable and hard to manage. This update provides a number of bug fixes and flags to the existing snapshot management APIs, so that libvirt can provide all the snapshot features, as documented. Management applications can use system checkpoint snapshots for better control when rolling back to known stable states of a virtual machine.

BZ#677229

Previously, libvirt did not support attaching of interfaces to an inactive virtual machine by using the "virsh attach-interface" command. Users had to use workarounds, for example editing the whole domain by executing "virsh edit". This update adds support for attaching interfaces even to inactive virtual machines. As a result, users do not need to use the workarounds, but can use virsh directly.

BZ#727474

Previously, libvirt used an improper separator (comma) in the "lvs" command. This caused the regular expression, which is used to parse the "lvs" output, to not function correctly. In addition, libvirt did not use the right mechanism to format multiple XML "devices" elements for multiple device paths of a striped volume. As a consequence, creation of any logical pool failed for LVM volume groups with striped volumes. With this update, a different separator (hash) is used. Multiple device paths of a striped volume are parsed correctly and multiple XML "devices" elements are formated as expected. Users are now able to create logical pools which contain a striped volume, and get proper XML for the striped volume as well.

BZ#720269

If the source QEMU process was not able to connect to the destination process when migrating a QEMU domain, libvirt could report "undefined error". With this update, libvirt creates the connection to the destination QEMU process and makes QEMU use this pre-created connection. This allows libvirt to report meaningful errors if the connection attempt fails.

BZ#707257

If a NFS (Network File System) storage was configured to be accessible only by users from a supplementary group for a user whose identity was used to run QEMU processes, the libvirtd daemon in certain cases failed to access or create files on that storage. With this update, libvirtd properly initializes supplementary groups when changing identity to QEMU users and groups. This allows libvirtd to access and create such files.

BZ#698825

Previously, it was not possible to maximize the performance of a KVM guest using memory binding on a NUMA (Non-Uniform Memory Access) host if the guest was started by libvirt. This update introduces new XML definitions to support NUMA memory policy configuration. Users can now specify the NUMA memory policy by using the guest XML definitions. The performance can be adjusted by NUMA memory binding.

BZ#704144

The libvirt library uses the "boot=on" option to determine which disk is bootable. The previous version of the qemu-kvm utility did not support this option, and libvirt could not use it. As a consequence, when an IDE disk was added as the second storage with a virtio being set up as the first one by default, the operating system tried to boot from the IDE disk rather than the virtio disk and either failed to boot with the "No bootable disk" error message, or the system booted whatever operating system was on the IDE disk. With this update, the boot configuration is translated into bootindex, which provides control over which device is used for booting a guest operating system.

BZ#751900

Prior to this update, when a QEMU migration to a file was triggered, libvirt temporarily set the migration bandwith to "unlimited" in an attempt to speed up saving of the state of the virtual machine. A limitation in QEMU caused QEMU not to return from the migrate command until the migration itself was complete. This locked out the QEMU monitor response loop and the migration to file process could not be interrupted. With this update, migration to file can be monitored for progress or interruptions. Now, libvirt no longer ignores job info or abort commands during the migration to file process.

BZ#738970

The virsh(1) man page did not mention detailed information about the drivers used for the "attach-disk" command with QEMU domains. If the command on a QEMU domain failed with an incorrect driver, users were unaware of what driver name should be used with QEMU. To fix this problem, the manual page now specifies what the "driver" parameter can contain.

BZ#693203

Running the "virsh list" command could become unresponsive when a QEMU process tracked by the libvirtd daemon did not respond to the monitor command. With this update, "virsh list" no longer requires interaction with running QEMU processes and can therefore list all domains even if a guest becomes unresponsive.

BZ#691830

If the user wanted to take a screenshot of a running virtual machine, the user had to use other tools (for example, virt-manager). A new libvirt API, virDomainScreenshot, is provided with this update, and allows users to take screenshots if the hypervisor supports it. Now, users no longer need to use third-party tools to take screenshots, but can use libvirt directly.

BZ#682237

SPICE (the Simple Protocol for Independent Computing Environments) supports multiple compression settings for audio, images and streaming. With this update, the libvirt XML schema is extended to support these kinds of settings so that users can set SPICE compression options directly in libvirt.

BZ#682084

Previously, libvirt did not support virtual CPU pinning on inactive virtual machines by running the "virsh vcpupin" command. Users had to use workarounds instead. With this update, libvirt now supports virtual CPU pinning on inactive virtual machines. Users no longer need to use workarounds but can use virsh directly.

BZ#681458

Previously, libvirt did not support attaching devices to an inactive virtual machine by running the "virsh attach-device" command. Users had to use workarounds, for example had to edit the whole domain using "virsh edit". With this update, libvirt provides enhanced support for attaching devices even to inactive virtual machines. User no longer need to use their workarounds but can use virsh directly.

BZ#727088

Previously, the new storage type added to libvirt was not fully supported. As a consequence, directory type storage volumes were reported to be file storage volumes. The new volume type has been added to the public API. The volume type is now correctly reported and displayed in associated tools.

BZ#641087

Users were allowed to change the domain's CPU affinity dynamically in libvirt, however there was no persistent XML provided, and the settings were lost on the next domain start. This update introduces a new XML to support the persistent configuration of domain's CPU affinity. Also new flags ("--live, "--config", and "--current") are introduced for the "virsh vcpupin" command. Now, the domain's CPU affinity persists across the next start.

BZ#730750

Previously, libvirt attempted to load a managed save file instead of starting a domain from the beginning, even if the managed save file was damaged and could not be loaded. This could confuse users who were not aware of the problem. This update introduces a new command, "virsh start --force-boot", as well as improved logic which ensures that a managed save file is not loaded if it is corrupted. Use of managed save images no longer cause confusion.

BZ#728153

If both the SysV init and upstart scripts were installed, and the libvirtd daemon was managed by upstart, the SysV init script was unaware of this. As a consequence, the SysV init script reported confusing error messages. The user was unable to restart the daemon by using the SysV init script, and was also unaware of the fact, that libvirtd was managed by upstart. With this update, the SysV init script checks whether libvirtd is managed by upstart. In the positive case, the user is advised to use the upstart tools to manage libvirtd. Users are now able to restart the libvirtd daemon while using upstart.

BZ#728428

When restarting the libvirtd daemon, libvirt reloaded the domain configuration from the status XML if the XML existed (the domain was running). However, the original domain configuration was not recorded and the domain configuration could not be restored to the original one. As a consequence, the nonpersistent attached devices still existed after restarting libvirtd. With this update, the original

domain configuration is recorded by assigning the persistent domain configuration to the newDef method if it's NULL and the domain is running. The nonpersistent attached devices no longer exist if libvirtd is restarted.

BZ#728654

The broken configuration file caused the libvirtd daemon to exit silently, with no error messages logged or any other indication of a problem. This could have confused the user as a consequence. Error handling messages have been added to the early start phases of libvirtd. Errors which occur during the start are now printed and logged.

BZ#678027

Previously, the DMI (Desktop Management Interface) data was not present on all architectures. Running the "virsh sysinfo" command failed on certain architectures because the DMI data was obtained from the missing /sys/devices/virtual/dmi tree. With this update, the DMI information is no longer fetched on non-Intel architectures. As a result, running the "virsh sysinfo" command works as expected.

BZ#730244

Previously, an invalid variable was used to construct error messages. If a migration command failed, the error message reported the remote URI to be "(null)" instead of the requested migration URI. The reason why the command failed was therefore unknown to the user. This update implements the correct variable which contains the migration URI. As a result, the correct migration URI is now reported if an error occurs.

BZ#667631

The monitor command in QEMU that provides migration information for SPICE was modified. As a consequence, libvirt was unable to send the migration information to SPICE, the session failed, and the migration terminated. This update modifies libvirt to adapt to the new monitor command. As a result, users can now perform a successful migration.

BZ#667624

The monitor command in QEMU that is used to change passwords for VNC and SPICE sessions was changed. As a consequence, libvirt was unable to set any password. This update modifies libvirt to adapt to the new command. As a result, users can successfully set passwords for VNC and SPICE sessions.

BZ#667620

Because QEMU changed the format of SPICE events, libvirt was not able to resend these event to users. This update modifies libvirt to adapt to the new format. As a result, SPICE events are successfully passed to users through libvirt.

BZ#589922

In certain cases, usually when the virt_use_nfs_selinux boolean was not set, SELinux policies prevented qemu from opening a disk image. As a consequence, qemu refused to start. This update provides a verbose error message which advises the user to set virt_use_nfs_selinux in the aforementioned scenario.

BZ#697742

Previously, libvirt did not remove the managed save file if a domain was undefined. When the user installed a new guest after destroying and undefining the previous one, the managed save file for the previous guest was still present, and the new guest failed to start because it would use a managed

save file with the same name. This update introduces a new API, virDomainUndefineFlags, which allows users to specify flags (for example, "virsh undefine --managed-save"). The managed save file can now be successfully removed. If the user does not specify any option, a comprehensive error message provides additional information.

BZ#722862

Previously, the virsh(1) man page contained duplicate documentation of the "iface-name" command, did not provide sufficient documentation of the "iface-mac" command, and contained certain inconsistent option names. The man page has been modified to provide correct descriptions.

BZ#692355

Previously, libvirt assigned PCI IDs to virtual devices as needed. As a consequence, migration of guests could fail in certain cases. With this update, libvirt reserves specific device IDs for virtual device types, notably 0x01 for IDE controllers and 0x02 for VGA devices. When migrating guests with other device types on these device IDs, users need to manually edit the guest XML files to reassign devices away from reserved IDs.

Enhancements

BZ#705814

The libvirt packages have been upgraded to upstream version 0.9.4, which introduces new APIs for libvirt and adds various enhancements over the previous version.

BZ#632760

In certain scenarios, users want to adjust the traffic of a virtual machine, its specific NIC (Network Interface Controller), or whole virtual network. Prior to this update, users often manually ran scripts to set up traffic shaping. This update extends the network and interface XML definitions. Now, users can set bandwidth limitation, or specify average peak and burst rates directly in libvirt.

BZ#692769

Users can limit virtual CPUs of a virtual machine by using control groups (cgroups). However, the appropriate QEMU process needs to be placed into a specific cgroup. Prior to this update, libvirt was missing this feature, and users had to use their own workarounds. With this update, libvirt can place a process into a cgroup, which can also be specified by using the XML definition of a virtual machine. As a result, users can now set virtual CPU bandwidth limits directly in libvirt.

BZ#711598

With SGA BIOS, it is possible to send boot messages to a serial line instead of a VNC/SPICE session. With this update, libvirt contains enhanced virtual machine XML descriptions so that users can set a serial line that allows the showing of boot messages. Boot messages are now displayed on the serial console as expected.

BZ#643947

The physical network interface configuration can be different on each host machine, even though each host is using the same logical network. This update adds a virtual switch abstraction to libvirt. Virtual machines can be configured identically on every host, even if the physical connectivity is different.

BZ#698340

Previously, libvirt did not support setting of the ioeventfd feature for virtio disks or interfaces. QEMU

could experience high CPU usage as a consequence. The support for this feature has been added in the XML definition of a virtual machine. Users can now enable the ioeventfd feature in order to lower CPU usage.

BZ#703851

The address used for listening for VNC connections to a libvirt guest was previously required to be an IP address. In cases where the guest migrates from one host to another, and the administrator wants the guest to be listening on a publicly visible interface, this address must be changed during migration. To make this change possible this update adds the option for specifying a listen network by name. Now, the guest can be migrated between the hosts, and its VNC listen address changes automatically as it migrates.

BZ#598792

The "--persistent" option for the "update-device" command was not implemented in virsh. Users experienced error messages saying that this feature was not supported. This update modifies libvirt to distinguish between the live and persistent XML definition of a virtual machine. Users can now change the definition of a virtual machine while the machine is running. The settings are applied after restarting the virtual machine.

BZ#632498

Running the "virsh dump" command against a virtual machine caused it to dump its memory. However, users often had to manually reboot the virtual machine after performing a dump. A new option, "--reset", has been implemented for "virsh dump", so that users can now use virsh instead of other tools.

BZ#677228

Previously, libvirt did not support attaching disks to an inactive virtual machine by using the "virsh attach-disk" command. Users had to use workarounds instead. This update provides enhanced support for attaching disks; disks can be attached even to inactive virtual machines. Now, users can use virsh directly instead of using workarounds.

BZ#569567

Changes made to host's network configuration by libvirt immediately and permanently modified host's configuration files. This caused the network to be unusable, and it was sometimes difficult to restore the original connectivity. This update adds new virsh commands, so that the current state of the network configuration can be saved and easily reverted.

BZ#634653

When migrating to a file, saving the state of a virtual machine led to creation of large files which filled the system cache. The system performance could therefore be affected. This update introduces the new "--bypass" option for operations that involve migration to file. This prevents the cache from being filled. Management application can now control large virtual machine state files.

All users of libvirt are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.150.2. RHBA-2011:1778 — libvirt bug fix update

Updated libvirt packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and

other operating systems. In addition, libvirt provides tools for remote management of virtualized systems. The library also provides nwfilter support for fine-grained filtering of the network traffic reaching guests managed by libvirt.

Bug Fix

BZ#754182

Previously, nwfilter support was dependent on the ability to execute scripts in the /tmp directory, which is considered unsafe. With this ability blocked, guests relying on the nwfilter component were not allowed to start. The underlying code has been modified so that nwfilter no longer requires to execute scripts in the /tmp directory.

All users of libvirt are advised to upgrade to these updated packages, which fix this bug. After installing these updated packages, libvirtd must be restarted. Use the "service libvirtd restart" command for this update to take effect.

4.150.3. RHBA-2012:0013 — libvirt bug fix and enhancement update

Updated libvirt packages that fix multiple bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems.

Bug Fixes

BZ#768469

This update forces all **libvirt** managed **KVM** guests with **`virtio`** drives to run with the **`scsi=off`** option. This will prevent SCSI requests in guests being passed to underlying block devices on the host; however, a separate bug is preventing **`scsi=off`** from working correctly. A malicious, privileged guest user could issue a **crafted request** that would still be passed to the underlying block device.

A future qemu-kvm update will correct the **`scsi=off`** functionality, blocking such crafted requests, and allowing CVE-2011-4127 to be mitigated before the kernel update is applied.

As **`scsi=off`** may break legitimate pass through of SCSI requests, this update also adds a new value for the device attribute in the disk XML element, **`lun`**. This type is like the default "disk" device, but will allow SCSI requests from guests to be passed to the underlying block device on the host. (Using the **`lun`** device attribute causes the guest to run with **`scsi=on`**.)

Note: After installing the RHSA-2011:1849 kernel update, it will not be possible for guests to issue SCSI requests on virtio drives backed by partitions or LVM volumes, even if **`device='lun'`** is used. It will only be possible to issue SCSI requests on virtio drives backed by whole disks.

Refer to Red Hat Knowledgebase 67869 for details about CVE-2011-4127.

BZ#769674

Due to an error in the **bridge network driver**, libvirt did not respect network configuration properly. Therefore, if a network was set with the **`forward`** element set to **`mode=bridge`**", libvirt incorrectly added **iptables** rules for such a network every time the **`libvirtd`** daemon was restarted and the

network was active. This could cause the network to become inaccessible. With this update, libvirt reloads iptables rules only if the **forward** element is set to **mode=route**, **mode=nat**, or **mode=none**.

BZ#769853

Previously, migration of a virtual machine failed if the machine had an ISO image attached as a CD-ROM drive and the ISO domain was inactive. With this update, libvirt introduces the new **startupPolicy** attribute for removable devices, which allows to mark CD-ROM and diskette drives as **optional**. With this option, virtual machines can now be started or migrated without removable drives if the source image is inaccessible.

BZ#770955

Under certain circumstances, a race condition between asynchronous jobs and query jobs could occur in the **QEMU** monitor. Consequently, after the **QEMU** guest was stopped, it failed to start again with the following error message:

```
error: Failed to start domain [domain name]
error: Timed out during operation cannot acquire state change lock
```

With this update, **libvirt** handles this situation properly, and guests now start as expected.

BZ#770957

The libvirt package was missing a dependency on the avahi package. The dependency is required due to **mDNS** support which is turned on by default. As a consequence, the **libvirtd** daemon failed to start if the libvirt package was installed on the system without **Avahi**. With this update, the dependency on avahi is now defined in the libvirt.spec file, and Avahi is installed along with libvirt.

BZ#770958

Due to several problems with security labeling, **libvirtd** became unresponsive when destroying multiple guest domains with disks on an unreachable **NFS** storage. This update fixes the security labeling problems and **libvirtd** no longer hangs under these circumstances.

BZ#770961

Previously, libvirt incorrectly released resources in the **macvtap** network driver in the underlying code for QEMU. As a consequence, after an attempt to create a virtual machine failed, a **macvtap** device that was created for the machine could not be deleted from the system. Any virtual machine using the same MAC address could not be created in such a case. With this update, an incorrect function call has been removed, and **macvtap** devices are properly removed from the system in the scenario described.

BZ#770966

Previously, libvirt defined a hard limit for the maximum number of domains (500) in **Python bindings**. As a consequence, the **vdsmd** daemon was unable to properly discover all virtual machines on the system with more than 500 guests. With this update, the number of domains is now determined dynamically and **vdsmd** correctly discovers all virtual machines.

Enhancements

BZ#759061

This update adds support for **VMware vSphere Hypervisor (ESXi) 5** installations.

BZ#770959

When shutting down, a virtual machine had changed its status from the **Up** state to the **Paused** state before it was shutdown. The **Paused** state represented the state when the guest had been already stopped, but **QEMU** was flushing its internal buffers and was waiting for **libvirt** to kill it. But this state change could confuse users so this update adds respective events and modifies libvirt to use the **shutdown** state. A virtual machine now moves from the **Up** to **Powering Down** and then to **Down** state.

All users of libvirt are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.150.4. RHBA-2012:0342 — libvirt bug fix update

Updated libvirt packages that fix four bugs are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems.

Bug Fixes

BZ#783453

Under certain circumstances, a rare race condition between the poll() event handler and the dmidecode utility could occur. This race could result in dmidecode waiting indefinitely to perform a read operation on the already closed file descriptor. As a consequence, it was impossible to perform any tasks for virtualized guests using the libvirtd management daemon, or perform certain tasks using the virt-manager utility, such as creating a new virtual machine. This update modifies the underlying code so that the race condition no longer occurs and libvirtd and virt-manager work as expected.

BZ#784785

Previously, when libvirt tried to attach certain SR-IOV (Single Root I/O Virtualization) devices to virtual guests, this attempts failed with the "Unable to reset PCI device" error messages. This patch modifies the underlying code so that these PCI devices can now be successfully attached to guests.

BZ#787620

When migrating a QEMU domain and using SPICE for a remote display, the migration was failing and the display was erratic under certain circumstances. This was happening because with the incoming migration connection open, QEMU was unable to accept any other connections on the target host. With this update, the underlying code has been modified to delay the migration connection until the SPICE client is connected to the target destination. The guest domains can now be successfully migrated without disrupting the display during the migration.

BZ#790779

Previously, if the libvirt package was built with avahi support, libvirt required the avahi package to be installed on the system as a prerequisite for its own installation. If the avahi package could not be installed on the system due to security concerns, installation of libvirt failed. This update modifies the libvirt.spec file to require only the avahi-libs package. The libvirt package is now successfully installed and libvirtd starts as expected.

All users of libvirt are advised to upgrade to these updated packages, which fix these bugs. After installing these updated packages, libvirtd must be restarted. Use the "service libvirtd restart" command for this update to take effect.

4.150.5. RHBA-2012:0419 — libvirt bug fix update

Updated libvirt packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems.

Bug Fixes

BZ#798177

If the user attempted to connect locally as a non-root user to the libvirtd daemon (using "qemu:///user"), the ".libvirt" directory was not created in the home directory. As a consequence, non-root users failed to use libvirt. This update ensures that the directory is created, and libvirt now works as expected for non-root users.

BZ#798906

The localtime_r() function used in the libvirt code was not async signal safe, which caused child processes to enter a deadlock when attempting to generate a log message. As a consequence, the virsh utility became unresponsive. This update applies backported patches and adds a new API for generating log time stamps in an async-signal safe manner. The virsh utility no longer hangs under these circumstances.

All users of libvirt are advised to upgrade to these updated packages, which fix these bugs. After installing these updated packages, libvirtd must be restarted. Use the "service libvirtd restart" command for this update to take effect.

4.150.6. RHBA-2012:0500 — libvirt bug fix update

Updated libvirt packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems.

Bug Fix

BZ#806206

When a live migration of a guest was terminated abruptly (using the Ctrl+C key combination), the libvirt daemon could have failed to accept any future migration request of that guest with the following error message:

```
error: Timed out during operation: cannot acquire state change
lock
```

This update adds support for registering cleanup callbacks which are called for a domain when a connection is closed. The migration API is more robust to failures, and if a migration process is terminated, it can be restarted on a subsequent command.

All users of libvirt are advised to upgrade to these updated packages, which fix this bug. After installing these updated packages, libvirtd must be restarted. Use the "service libvirtd restart" command for this update to take effect.

4.150.7. RHBA-2012:0727 — libvirt bug fix update

Updated libvirt packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems.

Bug Fixes

BZ#826639

Due to a locking problem in one of the routines involved in the migration process, migrations could become unresponsive, for example, when repeatedly migrating a domain between two nodes. The locking problem has been fixed with this update, and migrating a guest is now successful in this scenario.

BZ#827047

Closing a file descriptor multiple times could, under certain circumstances, lead to a failure to execute the qemu-kvm binary. As a consequence, a guest failed to start. A patch has been applied to address this issue, so that the guest now starts successfully.

All users of libvirt are advised to upgrade to these updated packages, which fix these bugs.

4.151. LIBVIRT-CIM

4.151.1. RHBA-2011:1587 — libvirt-cim bug fix and enhancement update

An updated libvirt-cim package that fixes one bug and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The libvirt-cim package contains a Common Information Model (CIM) provider based on Common Manageability Programming Interface (CMPI). It supports most libvirt virtualization features and allows management of multiple libvirt-based platforms.

Bug Fix

BZ#728245

Prior to this update, libvirt-cim contained several defects for null variables. As a result, using null variables did not work as expected. This update resolves these defects and now null variables work as expected.

Enhancements

BZ#633337

With this update, libvirt-cim supports libvirt networking Access Control Lists (ACL).

BZ#712257

This update aprovides read-only access to ensure that the remote CIM access cannot modify the system state. This is useful when CIM is used only for monitoring and other software is used for virtualization management.

All libvirt-cim users are advised to upgrade to this updated package, which fixes this bug and adds these enhancements.

4.152. LIBVIRT-QMF

4.152.1. RHBA-2012:0525 — libvirt-qmf bug fix update

Updated libvirt-qmf packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The libvirt-qmf packages provide an interface with libvirt using Qpid Management Framework (QMF), which utilizes the Advanced Message Queuing Protocol (AMQP). AMQP is an open standard application layer protocol providing reliable transport of messages.

Bug Fix

BZ#807931

Qpid APIs using the libpidclient and libpidcommon libraries are not application binary interface (ABI) stable. These dependencies have been removed so that Qpid rebuilds do not affect the libvirt-qmf packages.

All users of libvirt-qmf are advised to upgrade to these updated packages, which fix this bug.

4.153. LIBVORBIS

4.153.1. RHSA-2012:0136 — Important: libvorbis security update

Updated libvorbis packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The libvorbis packages contain runtime libraries for use in programs that support Ogg Vorbis. Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format.

Security Fix

CVE-2012-0444

A heap-based buffer overflow flaw was found in the way the libvorbis library parsed Ogg Vorbis media files. If a specially-crafted Ogg Vorbis media file was opened by an application using libvorbis, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of libvorbis should upgrade to these updated packages, which contain a backported patch to correct this issue. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.154. LIBXKLAVIER

4.154.1. RHBA-2012:0005 — libxklavier bug fix update

An updated libxklavier package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The libxklavier library provides a high-level API for the X Keyboard Extension (XKB) that allows extended keyboard control. This library supports X.Org and other commercial implementations of the X Window system. The library is useful for creating XKB-related software, such as layout indicators. This update fixes the following bug:

BZ#767267

Due to the way how the NoMachine NX Free Edition server implements XInput support, an attempt to log into the server using an NX or VNC client triggered an XInput error that was handled incorrectly by the libxklavier library. Consequently, the GNOME Settings Daemon (gnome-settings-daemon) was terminated with signal 6 (SIGABRT). To resolve this problem, the XInput error handling routine in the libxklavier library has been modified. The library now ignores this error and gnome-settings-daemon runs correctly under these conditions.

All users of libxklavier are advised to upgrade to this updated package, which fixes this bug.

4.155. LIBXML2

4.155.1. RHSA-2011:1749 — Low: libxml2 security and bug fix update

Updated libxml2 packages that fix several security issues and various bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libxml2 library is a development toolbox providing the implementation of various XML standards. One of those standards is the XML Path Language (XPath), which is a language for addressing parts of an XML document.

Security Fixes

CVE-2011-0216

An off-by-one error, leading to a heap-based buffer overflow, was found in the way libxml2 parsed certain XML files. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-1944

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way libxml2 parsed certain XPath expressions. If an attacker were able to supply a specially-crafted XML file to an application using libxml2, as well as an XPath expression for that application to run against the crafted file, it could cause the application to crash or, possibly, execute arbitrary code.

CVE-2010-4008, **CVE-2010-4494**, **CVE-2011-2821**, **CVE-2011-2834**

Multiple flaws were found in the way libxml2 parsed certain XPath expressions. If an attacker were able to supply a specially-crafted XML file to an application using libxml2, as well as an XPath expression for that application to run against the crafted file, it could cause the application to crash.

Note: Red Hat does not ship any applications that use libxml2 in a way that would allow the CVE-2011-1944, CVE-2010-4008, CVE-2010-4494, CVE-2011-2821, and CVE-2011-2834 flaws to be exploited; however, third-party applications may allow XPath expressions to be passed which could trigger these flaws.

Red Hat would like to thank the Google Security Team for reporting the CVE-2010-4008 issue. Upstream acknowledges Bui Quang Minh from Bkis as the original reporter of CVE-2010-4008.

Bug Fixes

BZ#732335

A number of patches have been applied to harden the XPath processing code in libxml2, such as fixing memory leaks, rounding errors, XPath numbers evaluations, and a potential error in encoding conversion.

All users of libxml2 are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.155.2. RHSA-2012:0018 — Important: libxml2 security update

Updated libxml2 packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libxml2 library is a development toolbox providing the implementation of various XML standards.

Security Fixes

CVE-2011-3919

A heap-based buffer overflow flaw was found in the way libxml2 decoded entity references with long names. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-3905

An out-of-bounds memory read flaw was found in libxml2. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash.

All users of libxml2 are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.155.3. RHSA-2012:0324 — Moderate: libxml2 security update

Updated libxml2 packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libxml2 library is a development toolbox providing the implementation of various XML standards.

Security Fix

CVE-2012-0841

It was found that the hashing routine used by libxml2 arrays was susceptible to predictable hash collisions. Sending a specially-crafted message to an XML service could result in longer processing time, which could lead to a denial of service. To mitigate this issue, randomization has been added to the hashing function to reduce the chance of an attacker successfully causing intentional collisions.

All users of libxml2 are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.156. LLDPAD

4.156.1. RHBA-2011:1604 — lldpad bug fix and enhancement update

An updated lldpad package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The lldpad package provides the Linux user space daemon and configuration tool for Intel's Link Layer Discovery Protocol (LLDP) agent with Enhanced Ethernet support.

The lldpad package has been upgraded to upstream version 0.9.43, which provides a number of bug fixes and enhancements over the previous version. (BZ#731407)

Bug Fixes

BZ#749057

The Brocade 8000 Fibre Channel Forwarder (FCF) switch with FabOs 6.4.2b failed to process the CEE TLV frame on fabric session startup (started by the llpad). As a consequence, the Brocade 8000 Fibre Channel Forwarder (FCF) switch with FabOs 6.4.2b terminated the connection and subsequent fabric logins failed when IEEE 802.1Qaz DCBX was enabled. With this update, the llptool utility can configure lldpad not to use the CEE TLV frame for the fabric session initiation (for the eth3 device, the initiator should issue the "lldptool -T -i eth3 -V IEEE-DCBX mode=reset" command) and the problem no longer occurs.

BZ#694639

The lldpad service triggered excessive timeout events every second. This caused the service to consume excess resources. Now, the lldpad service has been switched from polling-based to a demand-based model. This prevents excessive timeout event generation and ensures that the service consumes only the expected resources.

BZ#733123

The lldpad utility did not detect the maximum number of traffic classes supported by a device correctly. This resulted in an invalid or incorrect hardware configuration. Now, the utility detects the maximum number of traffic classes correctly.

BZ#720825, BZ#744133

The Edge Control Protocol (ECP) could not verify whether a port lookup was successful when running Virtual Discovery and Configuration Protocol (VDP) on bonded devices because VDP does not support bonded devices. As a consequence, the LLDP agent terminated unexpectedly with a segmentation fault. With this update, VDP is no longer initialized on bonded devices and the crash no longer occurs.

BZ#647211

The lldpad utility failed to initialize correctly on the Intel 82599ES 10 Gigabit Ethernet Controller (Niantic) with virtual functions enabled and returned a message that there were too many neighbors. With this update, lldpad initializes correctly and the problem no longer occurs.

BZ#735313

Prior to this update, a user with non-superuser permissions could start the lldpad service. With this update the lldpad init scripts have been modified and a user with non-superuser permissions can no longer start the service.

BZ#683837

The init script did not perform a line feed when returning the output of a service command. With this update, the init script has been recoded and the output of the service command is correct.

BZ#720730

The get_bcn() function returned without freeing the nlh variable, which caused a memory leak. The function has been modified and the memory leak no longer occurs.

BZ#741359

The lldpad daemon failed to detect that a NIC (Network Interface Card) had the offloaded DCBX (Data Center Bridging eXchange) stack implemented in its firmware. As a consequence, the lldp packets were send by both, the daemon and the NIC. With this update, the lldpad daemon no longer sends the packets if a NIC driver implements the offloaded DCBX stack.

BZ#749943

The lldpad utility incorrectly accessed memory. With this update, the utility accesses the memory correctly.

Enhancement

BZ#695550

The lldpad package now supports the 802.1Qaz standard (Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes).

Users are advised to upgrade to this updated lldpad package, which fixes these bugs and adds these enhancements.

4.156.2. RHBA-2012:0694 — lldpad bug fix update

Updated lldpad packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The lldpad packages provides the Linux user space daemon and configuration tool for Intel's Link Layer Discovery Protocol (LLDP) agent with Enhanced Ethernet support.

Bug Fix

BZ#822377

The lldpad tool is initially invoked by initrd during the boot process to support Fibre Channel over Ethernet (FCoE) boot from a Storage Area Network (SAN). The runtime lldpad init script did not kill lldpad before restarting it after system boot. Consequently, lldpad could not be started normally after system boot. With this update, the lldpad init script now contains the "-k" option to terminate the first instance of lldpad that was started during system boot.

All users of lldpad are advised to upgrade to these updated packages, which fix this bug.

4.156.3. RHBA-2012:0728 — lldpad bug fix update

Updated lldpad packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The lldpad packages provide the Linux user space daemon and configuration tool for Intel's Link Layer Discovery Protocol (LLDP) agent with Enhanced Ethernet support.

Bug Fix

BZ#828683

Previously, dcbtool commands could, under certain circumstances, fail to enable the Fibre Channel over Ethernet (FCoE) application type-length-values (TLV) for a selected interface during the installation process. Consequently, various important features might have not been enabled (for example priority flow control, or PFC) by the Data Center Bridging eXchange (DCBX) peer. To prevent such problems, application-specific parameters (such as the FCoE application TLV) in DCBX are now enabled by default.

All users of lldpad are advised to upgrade to these updated packages, which fix this bug.

4.157. LOHIT-ASSAMESE-FONTS

4.157.1. RHEA-2011:1138 — lohit-assamese-fonts enhancement update

An updated lohit-assamese-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-assamese-fonts package provides a free Assamese TrueType/OpenType font.

Enhancement

BZ#691284

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-assamese-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.158. LOHIT-BENGALI-FONTS

4.158.1. RHEA-2011:1141 — lohit-bengali-fonts enhancement update

An updated lohit-bengali-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-bengali-fonts package provides a free Bengali TrueType/OpenType font.

Enhancement

BZ#691285

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-bengali-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.159. LOHIT-GUJARATI-FONTS

4.159.1. RHEA-2011:1134 — lohit-gujarati-fonts enhancement update

An updated lohit-gujarati-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-gujarati-fonts package provides a free Gujarati TrueType/OpenType font.

Enhancement

BZ#691287

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-gujarati-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.160. LOHIT-KANNADA-FONTS

4.160.1. RHEA-2011:1140 — lohit-kannada-fonts enhancement update

An updated lohit-kannada-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-kannada-fonts package provides a free Kannada TrueType/OpenType font.

Enhancement

BZ#691289

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-kannada-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.161. LOHIT-MALAYALAM-FONTS

4.161.1. RHEA-2011:1136 — lohit-malayalam-fonts enhancement update

An updated lohit-malayalam-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-malayalam-fonts package provides a free Malayalam TrueType/OpenType font.

Enhancement

BZ#691290

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-malayalam-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.162. LOHIT-ORIYA-FONTS

4.162.1. RHEA-2011:1137 — lohit-oriya-fonts enhancement update

An updated lohit-oriya-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-oriya-fonts package provides a free Oriya TrueType/OpenType font.

Enhancement

BZ#691293

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-oriya-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.163. LOHIT-PUNJABI-FONTS

4.163.1. RHEA-2011:1135 — lohit-punjabi-fonts enhancement update

An updated lohit-punjabi-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-punjabi-fonts package provides a free Punjabi TrueType/OpenType font.

Enhancement

BZ#691294

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-punjabi-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.164. LOHIT-TAMIL-FONTS

4.164.1. RHEA-2011:1139 — lohit-tamil-fonts enhancement update

An updated lohit-tamil-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-tamil-fonts package provides a free Tamil TrueType/OpenType font.

Enhancement

BZ#691295

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-tamil-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.165. LOHIT-TELUGU-FONTS

4.165.1. RHEA-2011:1142 — lohit-telugu-fonts enhancement update

An updated lohit-telugu-fonts package which adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-telugu-fonts package provides a free Telugu TrueType/OpenType font.

Enhancement

BZ#691297

Unicode 6.0, the most recent major version of the Unicode standard, introduces the Indian Rupee Sign (U+20B9), the new official Indian currency symbol. With this update, the lohit-telugu-fonts package now includes a glyph for this new character.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

4.166. LSOF

4.166.1. RHEA-2011:1753 — lsof enhancement update

An updateed lsof package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lsof package provides the LiSt Open Files (LSOF) tool to list information about files that are open and running on a Linux/UNIX system.

Enhancement

BZ#671480

This enhancement update adds the new option +|-e s to lsof which exempts file systems with the path name "s" from being subjected to kernel function calls that might block. Note, that only the first +|-e argument is processed and the rest is ignored.

All users of lsof are advised to upgrade to this updated package, which add this enhancement.

4.167. LUCI

4.167.1. RHBA-2011:1510 — luci bug fix and enhancement update

An updated luci package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The luci package contains a web-based high availability cluster configuration application.

Bug Fixes

BZ#599074

When defining a cluster and checking the **`Use the Same Password for All Nodes`** box, an error message, saying that the user did not enter a password for any of the clusters except the first one, appeared after the user had submitted the changes. The password synchronization was triggered only once by checking the box. As a consequence, if no password was entered before checking the box, none could be copied into the other password fields. This update fixes the problem so that filling any single password field in the form causes the password to be correctly submitted for every node affected.

BZ#632536

Upgrading or downgrading the luci package could result in SELinux AVC (Security-Enhanced Linux Access Vector Cache) denials due to the python applications searching for local customizations in the **`Home`** directory. With this update, Python's paste tool now uses the ***`-Es`*** flag, and so avoids this behavior.

BZ#639121

If changes were made in any of the lightbox dialog boxes, a dialog box was hidden instead of being reset after it had been closed. As a consequence, when the dialog box was reopened, it was in the same state as before closing. The only way to reset the state of the dialog box was to refresh the

page in the browser. Now, when the user closes the existing dialog box, the page refreshes automatically instead of trying to recreate the initial state.

BZ#643488

Previously, titles of certain dialog boxes in the **luci** UI contained inconsistent character casing. Now, character casing is consistent in all titles.

BZ#703574

Previously, **luci** did not provide any way to back up or restore the content of the database. With this update, the content of the **luci** database located in **`/var/lib/luci/data/luci.db`** can be fully backed up and restored.

BZ#705111

In **luci**, when editing a failover domain that had both the**`Restricted`** and **`Prioritized`** boxes unchecked, adding of a node had no effect. The operation appeared to be successful, however the node was not added to the domain in the cluster.conf file. With this update, nodes can be successfully added to the failover domain. Removing nodes from the failover domain now works correctly as well.

BZ#705884

Previously, a bug in **luci** resulted in **luci** not being able to parse lines which contained the name of a service ending with the ".1" suffix. As a consequence, when importing a cluster, **luci** logged an error or displayed the Error 500 message in the browser. This update removes the bug and **luci** can now parse names ending with ".1" correctly.

BZ#707918

When the user created a file system resource and then tried to edit any field of a cluster service, an error message was printed and the changes were not applied. With this update, the source code is modified so that the changes are successfully applied.

BZ#708205

Previously, the **`Run Exclusive`** checkbox on the administration panel for a service group did not correspond to the configuration of this service group's entry in the **`cluster.conf`** file. The **`Run Exclusive`** option was enabled in **luci** by default, without it being manually enabled, and services could therefore become exclusive without users knowing about it. Now, **luci** is modified to correspond with the **`cluster.conf`** file: if the ***`Run Exclusive`*** option is not enabled, the checkbox is not checked.

BZ#711625

Due to **luci** not showing the migrate action for virtual machines, the Error 500 error message could appear when attempting to create a cluster of KVM (Kernel-based Virtual Machine) guests. With this update, **luci** is modified so that the services can be started and edited successfully.

BZ#714285

Prior to this update, the stop/start service was performed instead of migration when migrating a virtual machine by choosing the **`Migrate to node...`** option in the drop down menu on the Service Details page. With this update, the source code is modified to successfully complete the migration of virtual machines using the web interface.

BZ#718355

Prior to this update, if **`Log debugging messages`** and **`Log messages to log file`** were

enabled in the Logging page and the user entered a file path in the textbox below, the Error 500 message appeared. The changes to logging could not be submitted as a consequence. This problem has been fixed and changes to logging are submitted correctly.

BZ#729730

Prior to this update, **luci** served web pages and XHTML documents for most of the web browsers with the "application/xhtml+xml" content type and with "application/xml and "text/html" as failback. Web pages for the Internet Explorer browser were consistently served with the "text/html" content type. As a consequence, users were unable to open the URL of the luci server using Internet Explorer 8.0 and an error message appeared instead. With this update, web pages are permanently served with the "text/html" content type. The login page shows up correctly and users are able to log in.

BZ#733084

When trying to save an empty value for an option that used to be non-empty before instead of removing such option from the cluster.conf file, it was saved as the previous non-empty value. If the user attempted to clear options for a virtual machine service that he had been configured, **luci** did not save configuration for the service and it was therefore impossible to clear them using only the web interface. This problem has been fixed and the options are now cleared properly.

BZ#733797

Previously, **luci** did not start a service on a preferred node. When the user chose a service with a failover domain on the Service Groups page, a service started on the first node even if the user did not choose the first node as the preferred one. Now, the Submit button is used instead of a link for the headers_detail form and thus fixes the problem.

Enhancements

BZ#522005

The previous version of **luci** did not provide any role-based access control system. With this update, **luci** contains a new system for managing user roles. Multiple users can now gain various privileges for managing or accessing clusters.

BZ#671285

Now, a warning message is displayed when the user logs in for the first time in the **luci** UI. The text warns users about possible problems related to managing clusters using the UI with no further knowledge of clustering.

BZ#664036

This update provides a confirmation dialog box, which appears when removing cluster nodes or the whole cluster by selecting all the nodes and clicking the Delete button.

BZ#705072

This update adds support for the new **`fence_vmware`** fence agent.

Users of luci are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.168. LVM2

4.168.1. RHBA-2011:1522 — lvm2 bug fix and enhancement update

Updated lvm2 packages that fix several bugs and add three enhancements are now available for Red Hat Enterprise Linux 6.

The lvm2 packages contain support for Logical Volume Management (LVM).

Bug Fixes

BZ#743112

Due to locking errors, multiple failed cmirror devices were unable to be replaced. With this update, the underlying source code has been modified to address this issue, and the aforementioned devices are correctly replaced should a failure occur.

BZ#696251

Prior to this update, extending a mirror volume beyond available extents while using the *cling by tags* allocation policy did not work properly. Normally, such an action returns an error message informing the user that there are insufficient allocatable extents for use. However, this check failed and caused a volume to be corrupted. Because the allocation code has been revised, restructured, and made more robust, the problematic scenario with extending mirror volumes while using the *cling by tags* policy no longer occurs.

BZ#684083

While performing extensive I/O operations in the background, the **pvmove** command could become unresponsive. With this update, the underlying source code has been modified to address this issue, and the **pvmove** command no longer hangs.

BZ#733320

When a striped logical volume was resized with the **lvresize** command, the size was rounded down to the stripe boundary. This could pose a problem when shrinking the volume with a file system on it. Even if a user determined the new size so that the file system did fit entirely onto the volume, and resized the volume, the alignment done by the **lvresize** command might have cut off a part of the file system, causing it to become corrupted. This update fixes the rounding for striped volumes so that a volume is never reduced more than requested.

BZ#594525

Prior to this update, placing mirror legs on different physical devices with the **lvcreate --alloc anywhere** command did not guarantee placement of data on different physical devices. With this update, the above command tries to allocate each mirror image on a separate device first before placing it on a device that is already used.

BZ#737087

If the **lvcreate** command was used with large physical volumes while using **%FREE**, **%VG**, **%PVS** or **%ORIGIN** for size definition, the resulting LV size was incorrectly calculated. This was caused by an integer overflow while calculating the percentages. This update provides a better way of calculating the sizes, by using proper typecasting, so that the overflow no longer occurs.

BZ#715190

Several LVM locking error and warning messages were returned during the system start-up which were caused by cluster locking (configured globally in **/etc/lvm/lvm.conf**). At the early stage of the system start-up, when the early init script tries to activate any existing VGs, the cluster

infrastructure is still not initialized (as well as the network interface) and therefore cluster locking cannot be used and the system falls back to file-based locking instead, causing several misleading error and warning messages to be returned. With this update, these error and warning messages are suppressed during the system start-up, and the system falls back to usable locking mechanism silently.

BZ#712147

The **vgimportclone** script triggered a code path in LVM that caused it to access already-released memory when a duplicated PV was found. Consequently, the VG that contained such PV was found to be inconsistent and the process ended up with a failure to read the VG. This update fixes this failure by saving such problematic strings to a temporary buffer, and thus avoiding improper memory access.

BZ#697945

The cluster LVM daemon (**clvmd**) was crashing when attempting to create a high number of volume groups at once. This was caused by the limit set by the number of available file descriptors per process. While **clvmd** was creating pipes and the limit was reached under the pressure of high number of requests, **clvmd** did not return an error but continued to use uninitialized pipes instead, eventually causing it to crash. With this update, **clvmd** now returns an error message immediately if the pipe creation fails.

BZ#734193

When using striped mirrors, improper and overly-restrictive divisibility requirements for the extent count could cause a failure to create a striped mirror, even though it was correct and possible. The condition that was checked counted in the mirror count and the stripe count, though, only the stripe count alone was satisfactory. This update fixes this, and creating a striped mirror no longer fails.

BZ#732142

Before, an improper activation sequence was used while performing an image split operation. That caused a device-mapper table to be loaded while some of processed devices were known to be suspended. This has been fixed and the activation sequence has been reordered so that the table is always loaded at proper time.

BZ#570359

Issuing an **lvremove** command could cause a failure to remove a logical volume. This failure was caused by processing an asynchronous udev event that kept the volume opened while the **lvremove** command tried to remove it. These asynchronous events are triggered when the **watch** udev rule is applied (it is set for device-mapper/LVM2 devices when using the udisks package that installs **/lib/udev/rules.d/80-udisks.rules**).

To fix this issue, the number of device open calls in read-write mode has been minimized and read-only mode is used internally if possible (the event is generated when closing a device that has the **watch** rule set and is closed after a read-write open).

Although this fixes a problem when opening a device internally within the command execution, the failure could still occur when using several commands quickly in a sequence where each one opens a device for read-write and then closes it immediately (for example in a script). In such a case, it is advisable to use the **udevadm settle** command in between.

BZ#695526

With this update, when using the **lvconvert** command, the Unable to create a snapshot of a locked|pvmove|mirrored LV error message has been changed to Unable to convert an LV into a snapshot of a locked|pvmove|mirrored LV. for clarity reasons.

BZ#711445

A hostname containing the slash character ("**/**") caused LVM commands to fail while generating an archive of current metadata. Because a hostname is a part of the temporary archive file name, a file path that was ambiguous was created, which caused the whole archive operation to fail. This update fixes this by replacing any slash character ("**/**") with a question mark character ("**?**") in the hostname string and then is used to compose the temporary archive file name.

BZ#712829

An issue was discovered when running several commands in parallel that activated or deactivated an LV or a VG. The symbolic links for LVs in **/dev** were created and removed incorrectly, causing them to exist when the device had already been removed or vice versa.

This problem was caused by the fact that during the activation there was no write lock held that would protect individual activation commands as a whole (there was no metadata change). Together with non-atomicity of checking udev operations, an improper decision was made in the code based on the already stale information. This triggered a part of the code that attempted to repair the symbolic links as a fallback action.

To fix this, these checks are no longer run by default, thus fully relying on **udev**. However, the old functionality can still be used for diagnosing other **udev** related problems by setting a new **verify_udev_operations** option found in the **activation** section of the **/etc/lvm/lvm.conf** file.

BZ#728157

This update removes the unsupported **--force** option from the **lvrename** manpage.

BZ#743932

With this update, the **vgsplit** command is now able to split a volume group containing a mirror with mirrored logs.

Enhancements

BZ#623808

Prior to this update, it was not possible to create a PV object with all properties calculated (for example, the PE start value) without a need to write the PV label on the disk while using an LVM2 library (**lvm2app**). This has been changed so that the PV label is written out later in the process as a part of the **lvm_vg_write** call, making it possible to calculate all PV properties and query them without actually writing the PV label on the disk.

BZ#651493

This update adds support for issuing *discards* (TRIM) as part of **lvm2** operations.

BZ#729712

In Red Hat Enterprise Linux 6.2, support for MD's RAID personalities has been added to LVM as a Technology Preview. For more information about this feature, refer to the Red Hat Enterprise Linux 6.2 Release Notes.

Users are advised to upgrade to these updated lvm2 packages, which resolve these issues and add these enhancements.

4.169. MAILCAP

4.169.1. RHBA-2011:1118 — mailcap bug fix update

An updated mailcap package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The mailcap package contains the mailcap file, which is used by the metamail program. Metamail reads the mailcap file to determine how it should display non-text or multimedia material. mailcap associates a particular type of file with a particular program that a mail agent or other program can call in order to handle the file. Mailcap should be installed to allow certain programs to be able to handle non-text files.

Bug Fix

BZ#610793

Prior to this update, the mime.types database did not contain the WebM MIME type (video/webm). The problem has been resolved in this update by including the MIME type in the database.

All users of mailcap are advised to upgrade to this updated package, which fixes this bug.

4.170. MAILMAN

4.170.1. RHBA-2011:1275 — mailman bug fix update

An updated mailman package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

Mailman is a program used to help manage email discussion lists.

Bug Fixes

BZ#704699, BZ#703389

Previously, a number of Python scripts and subdirectories in the /usr/lib/mailman/ directory were group writable. As a result, the respective files and subdirectories could have been changed not only by the owner, but also by other users in the same user group. This undesired behavior has been resolved in this update so that only the owner can now change the files and subdirectories.

BZ#684622

Because of a bug in the brp-python-compile script file, unnecessary /etc/mailman/mm_cfg.pyc and /etc/mailman/mm_cfg.pyo files were generated under certain circumstances. As a result, the Mailman build process could have failed. This update fixes the aforementioned bug by compiling Python script files manually so that the build process no longer fails.

BZ#636825

In accordance with current guidelines, all Python executable files have been updated to use the Python executable file directly, that is the "#!/usr/bin/python" string instead of "#!/usr/bin/env python".

All users of mailman are advised to upgrade to this updated package, which fixes these bugs.

4.171. MAN-PAGES-JA

4.171.1. RHBA-2011:0962 — man-pages-ja bug fix update

An updated man-pages-ja package that fixes multiple bugs is now available for Red Hat Enterprise Linux 6.

The man-pages-ja package contains Japanese translations of the Linux Documentation Project man pages.

Bug Fixes

BZ#579641

Prior to this update, the man-pages-ja package did not contain the Japanese translations of the man pages of the "halt", "init", "poweroff", "reboot", "runlevel", "shutdown", and "telinit" commands. With this update, the aforementioned man page translations have been added.

BZ#682122

Prior to this update, the Japanese translation of the getpriority(2) man page contained a typo in the range of "nice values". This update corrects the typo.

BZ#699301

Prior to this update, the Japanese translation of the wall(1) man page contained a typo in the description of the message length limit. This update corrects the typo.

BZ#710704

Prior to this update, the Japanese translation of the tar(1) man page did not contain descriptions of the "--selinux" and "--no-selinux" options. With this update, the missing descriptions have been added.

All users of man-pages-ja are advised to upgrade to this updated package, which fixes these bugs.

4.172. MAN-PAGES-OVERRIDES

4.172.1. RHBA-2011:1571 — man-pages-overrides bug fix update

An updated man-pages-overrides package that fixes multiple bugs is now available for Red Hat Enterprise Linux 6.

[Updated 28 March 2012] This advisory has been updated with the correct description for bug 688543. The package included in this revised update has not been changed in any way from the package included in the original advisory.

The man-pages-overrides package contains a collection of manual (man) pages to complement other packages or update those contained therein.

Bug Fixes

BZ#615897

Previously, a manual page for the lsmsr utility was missing. This update adds the lsmsr(8) manual page.

BZ#656245

Previously, a manual page for the fattach function was missing. This update adds the fattach(2) manual page.

BZ#674423

Previously, a manual page for the recvmmsg call was missing. This update adds the recvmmsg(2) manual page.

BZ#728416

Previously, a manual page for the sendmmsg call was missing. This update adds the sendmmsg(2) manual page.

BZ#688543

Prior to this update, the lscfg(8), lsmcode(8), lsmsr(8), lsvio(8), and vpdupdate(8) manual pages did not document multiple lsvpd options. This update adds all missing options to the manual pages.

BZ#690187

Previously, manual pages for the cciss and hpsa utilities were missing. This update adds the cciss(4) and hpsa(4) manual pages.

BZ#730042

Previously, a manual page for the cpufreq-aperf utility was missing. This update adds the cpufreq-aperf(1) manual page.

BZ#709058

Previously, the ntp-keygen(8) manual page contained multiple typos. This update corrects these typos.

BZ#709274

Previously, the ntpq(8) manual page contained multiple typos. This update corrects these typos.

BZ#712256

Previously, the volume_key(8) manual page contained a typo. This update corrects this typo.

BZ#727526

Previously, the curl(1) manual page contained a typo. This update corrects this typo.

BZ#731690

Previously, multiple ecryptfs manual pages contained an incorrect link in the SEE ALSO section. With this update, the link is now fixed.

BZ#734836

Previously, the clock_gettime(2), clock_getres(2), and clock_nanosleep(2) manual pages did not mention the "-lrt" option. With this update, the "-lrt" option is now described in the corresponding manual pages.

BZ#698151

The host.conf(5) manual page contained a description for the unsupported "order" keyword. With this update, the description of the "order" keyword is removed.

BZ#742098

Previously, the nfs(5) manual page contained an inaccurate description of the "timeo" option. With this update, the description is now enhanced.

BZ#740670

Previously, the vsftpd.conf(5) manual page contained incorrect information about the default values of the "max_per_ip" option. With this update, the information is now fixed.

BZ#602228

With this update, the new multicast feature is now described in the brctl(8) manual page.

BZ#717770

With this update, the "single-request-reopen" option is now described in the resolv.conf(5) manual page.

BZ#723791

With this update, the new UMOUNT_NOFOLLOW flag is described in the umount(2) manual page.

BZ#694860

With this update, usage of SSSD in the nsswitch.conf file is now described in the nsswitch.conf(5) manual page.

BZ#719902

This update removes multiple manual pages from the original package.

All users of man-pages-overrides are advised to upgrade to this updated package, which fixes these bugs.

4.173. MATAHARI

4.173.1. RHBA-2011:1569 — matahari bug fix and enhancement update

Updated matahari packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The matahari packages provide a set of APIs for operating system management that are exposed to remote access over the Qpid Management Framework (QMF).

Bug Fixes

BZ#688193

Prior to this update, the matahari services agent could not monitor the status of a system service. As a consequence, matahari could not be used in high-availability (HA) environments where status monitoring is a requirement. With this update, the user of the services agent can specify the frequency for the status check and the matahari services agent can now provide service health information for applications such as HA.

BZ#714249

Prior to this update, the wrong CPU core count was returned when requesting the CPU core count from the matahari host agent. With this update, matahari and the supporting library, sigar, have been modified to ensure that the core count is not improperly affected by hyperthreading support. Now, the expected CPU core count is returned.

BZ#729063

Prior to this update, the host agent included only time related metadata when producing heartbeat events. As a consequence, it was problematic to associate heartbeat events with the host they originated from, especially in logs. With this update, the heartbeat events produced by the Host agent include the hostname and the hardware's Universally Unique Identifier (UUID) as additional metadata. Now, it is easier to associate the host agent heartbeat events with the host they originated from.

BZ#732498

Prior to this update, the data address for matahari QMF objects was inconsistent. As a consequence, the data address for some agents was the class name, for others it was a UUID. This update uses consistently the class name as the data address. Now, the data address across all matahari agents is consistent.

Enhancements

BZ#663468

Prior to this update, matahari only supported IBM eServer xSeries 366, AMD64 and Intel 64 architectures. This update adds support for PowerPC and IBM System z architectures as a Technology Preview.

BZ#688181

This update adds support for QMF to allow for kerberos authentication.

BZ#688191

With this update, matahari includes an agent for system configuration to support updating the system configuration with both puppet and augeas.

BZ#735419

Prior to this update, users could only specify a hostname or IP address. As a consequence, a dynamically updated list of brokers to connect to was not provided. With this update, matahari supports querying for DNS SRV records to determine the broker, or the list of brokers to connect to. Now administrators can use DNS SRV to control where matahari agents connect to.

All users of matahari are advised to install these packages, which fix these bugs and add these enhancements.

4.173.2. RHBA-2012:0511 — matahari bug fix update

Updated matahari packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The matahari packages provide a set of APIs for operating system management that are exposed to remote access over the Qpid Management Framework (QMF).

Bug Fix

BZ#806766

Qpid APIs using the libpidclient and libqpidcommon libraries are not application binary interface (ABI) stable. These dependencies have been removed so that Qpid rebuilds do not affect the matahari packages.

All users of matahari are advised to upgrade to these updated packages, which fix this bug.

4.174. MCELOG

4.174.1. RHEA-2011:1579 — mcelog enhancement update

An enhanced mcelog package is now available for Red Hat Enterprise Linux 6.

mcelog is a daemon that collects and decodes Machine Check Exception data on AMD64 and Intel 64 machines.

Enhancement

BZ#699592

This update enables full Predictive Failure Analysis (PFA) support in mcelog. Predictive Failure Analysis (PFA) is a technology for monitoring the probability of hard disk drive failure.

In addition, mcelog is now able to collect and log data by default upon package installation.

Users of mcelog are advised to upgrade to this updated package, which adds these enhancements.

4.175. MDADM

4.175.1. RHBA-2011:1520 — mdadm bug fix update

An updated mdadm package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The mdadm package contains a utility for creating, managing, and monitoring Linux MD (multiple disk) devices.

Bug Fixes

BZ#692261

The mdadm utility incorrectly detected an IMSM (Intel Matrix Storage Manager) RAID device that was in the **resync** status, as being in the **reshape** status. As a consequence, mdadm rejected to assemble the IMSM RAID device as an external data file is needed to reassemble a device in the **reshape** status. If booting from the IMSM RAID device, the boot process could fail under these circumstances. With this update, mdadm detects that an IMSM RAID device is in the **resync** mode, assembles the device correctly, and launches its synchronization.

BZ#694083

When an array was changing the RAID level from redundant to non-redundant, the mdmon monitoring tool failed to close. As a consequence, mdmon applied the initial structure to the new array and mdadm could terminate with a segmentation fault. With this update, the underlying code has been modified and mdmon closes under these circumstances.

BZ#702270

The resync progress of an array, which was already partially resynchronized, was reset to zero and the resync process was restarted. This occurred if a newly-assembled array requested resync and reset the progress of another array from the container which was already partially resynchronized. With this update, the underlying code has been modified and a degraded RAID continues its resync from the point it had reached on previous resynchronizing.

BZ#598513

The mdadm utility handled the udev incremental rules incorrectly. As a consequence, it failed to handle incremental assembly of RAID devices built on top of logical multipath devices and a RAID device configured on top of a multipath device did not assemble during the boot process. With this update, mdadm handles the udev incremental rules file correctly and such devices are assembled as expected.

BZ#733153

Due to unexpected attributes in RAID metadata, the assembly of a RAID device could fail and the device was not available to the system. With this update, the metadata attributes are ignored and the RAID device is assembled as expected during boot.

BZ#695336

The mdadm utility calculated the data disks number during a reshape restart incorrectly and due to this miscalculation could attempt to divide by 0. As a result, reassembly of a migrated array could cause a floating point exception. With this update, the underlying code has been modified and the number of data disks is calculated correctly.

BZ#694103

Buffer size used on double-degraded RAID6 devices was insufficient. As a result, the RAID recovery failed and mdadm terminated unexpectedly. This happened because the buffer could not write data back to a stripe size if the recovered stripe was larger than the original stripe and the buffer overran. With this update, mdadm checks the size of the requested buffer and allocates a larger buffer for the stripe under these circumstances, and the recovery of double-degraded RAID6 completes successfully.

BZ#694121

If an array was created using the **`--size`** option with no chunk size specified, the mdadm utility rounded the default chunk size incorrectly. With this update, the rounding process has been modified and arrays are created with the correct size alignment.

BZ#694779

When expansion or reshape of RAID0 volume was restarted, mdadm failed to assemble the array because it failed to restore a critical section of the backup file and exited with the following message:

```
mdadm: Failed to restore critical section for reshape - sorry
```

This happened because during the process, the RAID level for RAID0 devices is temporarily changed to RAID4; however, the Grow_restart() function called on restart did not allow any RAID level changes. With this update, the level change has been allowed and the problem no longer occurs.

BZ#609122, BZ#6674703

The udev scripts did not add encrypted devices to a RAID device because encrypted devices were ready only after they had been unlocked. As a consequence, a RAID device created on top of one or

more encrypted block devices failed to assemble. With this update, the underlying code has been changed and the script unlocks encrypted devices and add them to the respective RAID device as expected.

BZ#706500

Due to incorrect internal accounting of disks, the mdadm utility failed to re-add a disk, which was previously marked as faulty and removed. With this update, the underlying code has been modified and such disk is re-added as expected.

BZ#727212

The output of the **`mdstat --examine`** command contained incorrect status information. This happened because the DELAYED/PENDING status of a RAID device during resync was translated to an incorrect status. An upstream patch that fixes this bug has been applied and the **`mdstat --examine`** command now returns correct status information.

BZ#716413

Version 0.90 arrays have the metadata_version value set to NULL while newer versions set the metadata to the respective version. When the mdmonitor utility was restarted, it attempted to dereference the metadata value and terminated with a segmentation fault when the value was NULL. As a consequence, the RAID device became inaccessible. With this update, the NULL pointer dereference for metadata_version has been fixed.

BZ#694092

The mdadm tool did not handle expansion of arrays which were not chunk size aligned. This happened because mdadm left the array prepared for reshape when the array expansion returned a message that the new chunk size was not divisible by the component size, which could prevent the array from being reassembled again later on. This update applies an upstream patch, which checks the alignment before preparing the array for expansion. The mdadm tool now rejects expansion of an array with incorrect chunk size alignment and the array can be reassembled later.

Users are advised to upgrade to this updated mdadm package, which resolves these bugs.

4.176. MESA

4.176.1. RHBA-2011:1616 — mesa bug fix and enhancement update

Updated mesa packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Mesa provides a 3D graphics application programming interface (API) that is compatible with OpenGL (Open Graphics Library). It also provides hardware-accelerated drivers for many popular graphics chips.

The mesa packages have been upgraded to upstream version 7.11, which provides a number of bug fixes and enhancements over the previous version. (BZ#713772)

Bug Fixes

BZ#677470

Prior to this update, the OpenGL output was corrupted due to problems with the rendering in guests. This update modifies the software rendering so that the OpenGL output is no longer corrupted.

BZ#745686

Prior to this update,the nouveau gallium driver was wrongly included in the mesa-dri-drivers package which could lead to conflicts. This update corrects this error and removes the nouveau gallium driver from the package.

All Mesa users are advised to upgrade to these updated packages, which fix these bugs add these enhancements.

4.177. MICROCODE_CTL

4.177.1. RHEA-2011:1594 — microcode_ctl bug fix and enhancement update

An updated microcode_ctl package that fixes a bug and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The microcode_ctl package provides microcode updates for Intel and AMD processors.

Bug Fix

BZ#684009

A previous update introduced a memory leak when loading the updated microcode into memory prior to conversion of said microcode into a format suitable for the CPU. This update includes a corrected patch that de-allocates the memory correctly, ensuring memory does not leak.

Enhancements

BZ#696582

The Intel CPU microcode file has been updated to version 20110915, which is the most recent version of the microcode available from Intel.

BZ#682668

The AMD CPU microcode file version 20110111 is now included in the package.

Note that the system must be rebooted in order for these changes to take effect.

Users are advised to upgrade to this updated microcode_ctl package, which fixes this bug and adds these enhancements.

4.178. MINGETTY

4.178.1. RHBA-2011:1177 — mingetty bug fix update

An updated mingetty package that fixes three bugs is now available for Red Hat Enterprise Linux 6.

The mingetty program is a lightweight, minimalist getty program for use only on virtual consoles. The mingetty program is not suitable for serial lines (the mgetty program should be used in that case).

Bug Fixes

BZ#640933

Prior to this update, when mingetty was invoked with the "--chroot" option, mingetty did not change the working directory to the new root. Furthermore, mingetty continued even if setting constraints specified by the "--chroot", "--chdir", and "--nice" options failed. As a result, a user was able to escape from the changed root by using relative paths. Also, it was possible for a user to obtain a process with a different process priority. These problems have been resolved in this update so that the working directory is now changed to the new root directory, all failures are now recognized, and mingetty terminates with an error reported to the system log.

BZ#640940

Prior to this update, when invoking mingetty with a TTY name (a non-option position argument) that was longer than 39 ASCII characters, a buffer overflow occurred and the mingetty stack content could have become corrupted. This bug has been fixed in this update so that only the first 39 bytes (34 bytes in case of a relative path) from the TTY name are now copied.

BZ#651955

Prior to this update, when using a login name longer than 39 characters, such login name was silently refused and mingetty terminated. With this update, login names with the length up to the current runtime limit are now accepted; login names that are above the limit are refused, an error is reported to the system log, and mingetty terminates.

All users of mingetty should upgrade to this updated package, which fixes these bugs.

4.179. MINGW32

4.179.1. RHEA-2011:1751 — mingw32 enhancement update

Updated mingw32 packages that add two enhancements are now available for Red Hat Enterprise Linux 6.

The mingw32 packages provide the MinGW (Minimalistic GNU for Windows) development environment.

Enhancements

BZ#722878

The previous version of the mingw32 packages used GCC in version 4.4.3. This enhancement update upgrades base mingw32 packages and rebuilds all dependent packages to make sure they are in sync with the latest GCC version (4.4.6) that is available in Red Hat Enterprise Linux 6.

BZ#719866

In accordance with the latest packaging guidelines, all packages that contain debugging information now have the "mingw32-" prefix.

All users of mingw32 are advised to upgrade to these updated packages, which add these enhancements.

4.180. MINGW32-QPID-CPP

4.180.1. RHBA-2011:1740 — mingw32-qpid-cpp bug fix and enhancement update

An updated mingw32-qpid-cpp package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The mingw32-qpid-cpp package provides a message broker daemon that receives, stores, and routes messages using runtime libraries for AMQP client applications developed using Qpid C++. Clients exchange messages with an AMQP message broker using the Advanced Message Queuing Protocol (AMQP), an open standard application layer protocol.

The mingw32-qpid-cpp package has been upgraded to upstream version 0.12, which provides a number of bug fixes and enhancements over the previous version. (BZ#706994)

All users of mingw32-qpid-cpp are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.181. MKSH

4.181.1. RHBA-2011:0923 — mksh bug fix update

An updated mksh package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The mksh package provides the MirBSD version of the Korn Shell, which implements the ksh-88 programming language for both interactive and shell script use.

Bug Fix

BZ#712355

Prior to this update, the mksh package did not specify all requirements for RPM scriptlets. As a result, the requirements were not installed during the post install setup and the scriptlets were not able to work correctly. With this update, the bug has been fixed, and the mksh package now specifies the requirements and installs them as expected.

All users of mksh are advised to upgrade to this updated package, which fixes this bug.

4.182. MOD_NSS

4.182.1. RHBA-2011:1656 — mod_nss bug fix update

An updated mod_nss package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The mod_nss module provides strong cryptography for the Apache HTTP Server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

Bug Fixes

BZ#691502

When the NSS library was not initialized and mod_nss tried to clear its SSL cache on start-up, mod_nss terminated unexpectedly when the NSS library was built with debugging enabled. With this update, mod_nss does not try to clear the SSL cache in the described scenario, thus preventing this bug.

BZ#714154

Previously, a static array containing the arguments for launching the nss_pcache command was overflowing the size by one. This could lead to a variety of issues including unexpected termination. This bug has been fixed, and mod_nss now uses properly sized static array when launching nss_pcache.

BZ#702437

Prior to this update, client certificates were only retrieved during the initial SSL handshake if the NSSVerifyClient option was set to "require" or "optional". Also, the FakeBasicAuth option only retrieved Common Name rather than the entire certificate subject. Consequently, it was possible to spoof an identity using that option. This bug has been fixed, the FakeBasicAuth option is now prefixed with "/" and is thus compatible with OpenSSL, and certificates are now retrieved on all subsequent requests beyond the first one.

Users of mod_nss are advised to upgrade to this updated package, which fixes these bugs.

4.182.2. RHBA-2012:0394 — mod_nss bug fix update

An updated mod_nss package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The mod_nss module provides strong cryptography for the Apache HTTP Server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

Bug Fixes

BZ#800270, BZ#800271

The RHBA-2011:1656 errata advisory released a patch that fixed a problem of mod_nss crashing when clearing its SSL cache on startup without the NSS library initialized. However, that patch placed the fix in the improper location in the code, which caused a file descriptor leak in the Apache httpd daemon. With this update, the necessary fix has been relocated to the appropriate location in the code so that the problem is fixed and the file descriptor leak no longer occurs.

All users of mod_nss are advised to upgrade to this updated package, which fixes these bugs.

4.183. MOD_REVOCATOR

4.183.1. RHBA-2011:1769 — mod_revocator bug fix update

An updated mod_revocator package that fixes multiple bugs is now available for Red Hat Enterprise Linux 6.

The mod_revocator module retrieves and installs remote Certificate Revocation Lists (CRLs) into an Apache web server.

Bug Fixes

BZ#748579

Previously, the code for the httpd daemon shutdown was incorrect and the mod_revocator module did not shut down the httpd daemon when CRL (Certificate Revocation List) update failed on IA-32 architectures. With this update, the code has been fixed and httpd is now closed as expected when CRL update fails.

BZ#748577

Previously, the code for httpd shutdown was incorrect and the mod_revocator module did not shut down the httpd daemon when expired CRLs were fetched. With this update, the code has been fixed and httpd is closed as expected in this scenario.

BZ#749696

Due to an incorrect initialization size of a static array, the httpd daemon with mod_revocator failed to start on 64-bit PowerPC architectures. With this update, the size of the array has been modified and the httpd starts as expected under these circumstances.

BZ#746365

The httpd daemon with the mod_revocator module cannot be used as an HTTP client by default because the SELinux policy prevents such behavior. However, to acquire CRLs from a remote host, the httpd daemon needs to behave as an HTTP client to send HTTP messages to the host. If the behavior was not enabled, child processes of the httpd daemon terminated unexpectedly with segmentation faults when attempting to connect to a remote host. With this update, the underlying code has been changed and the segmentation faults no longer occur.

NOTE

To change the SELinux policy and enable httpd to request CRLs from a remote host, execute the "setsebool -P httpd_can_network_connect=1" command as root.

All users of mod_revocator are advised to upgrade to this updated package, which fixes these bugs.

4.184. MODULE-INIT-TOOLS

4.184.1. RHBA-2012:0366 — module-init-tools bug fix and enhancement update

An updated module-init-tools package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The module-init-tools package includes various programs needed for automatic loading and unloading of modules under 2.6 and later kernels, as well as other module management programs. Device drivers and file systems are two examples of loaded and unloaded modules.

Bug Fixes

BZ#787741

Previously, if the "override" keyword was present in the depmod.conf file without any parameters specified, the depmod utility terminated unexpectedly with a segmentation fault. A patch has been applied to ensure that the depmod utility no longer crashes and a syntax warning is displayed instead.

BZ#797183

Previously, on low-memory systems (such as low-memory high-performance infrastructure, or HPC, nodes or virtual machines), depmod could use excessive amount of memory. As a consequence, the depmod process was killed by the OOM (out of memory) mechanism, and the system was unable to boot. With this update, the free() function is correctly used on several places in the code so that so that depmod's memory consumption is reduced.

Enhancement

BZ#787748

This update adds the "backports" directory to the search path in the depmod.conf file, which is necessary to support integration of the compat-wireless package into kernel packages.

All users of module-init-tools are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.185. MYSQL

4.185.1. RHSA-2012:0105 — Important: mysql security update

Updated mysql packages that fix several security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

Bug Fixes

CVE-2011-2262, **CVE-2012-0075**, **CVE-2012-0087**, **CVE-2012-0101**, **CVE-2012-0102**, **CVE-2012-0112**, **CVE-2012-0113**, **CVE-2012-0114**, **CVE-2012-0115**, **CVE-2012-0116**, **CVE-2012-0118**, **CVE-2012-0119**, **CVE-2012-0120**, **CVE-2012-0484**, **CVE-2012-0485**, **CVE-2012-0490**, **CVE-2012-0492**

This update fixes several vulnerabilities in the MySQL database server. Information about these flaws can be found on the Oracle Critical Patch Update Advisory page.

These updated packages upgrade MySQL to version 5.1.61. Refer to the MySQL release notes for a full list of changes:

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-x.html

All MySQL users should upgrade to these updated packages, which correct these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

4.186. NAUTILUS

4.186.1. RHBA-2011:1203 — nautilus bug fix update

Updated nautilus packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The Nautilus file manager is a core component of the GNOME desktop project. It allows users to browse directories on local and remote file systems, preview files and launch applications associated with them. It is also responsible for handling the icons on the GNOME desktop.

Bug Fixes

BZ#616774

Previously, the "Volume is busy" dialog was not linked to any window, which led to the "Untitled window" item appearing on the taskbar when the user unmounted or ejected a device with one or more files opened. This update sets the dialog temporarily for the desktop window which automatically removes the taskbar item.

BZ#636881

Previously, an incorrect signal was emitted when the user changed the name of a bookmark created in Nautilus. As a consequence, the changes got lost and the new name was not written into the bookmark file. This has been fixed: the correct signal is now emitted and the bookmarks can be properly updated.

BZ#652607

Previously, Nautilus could close unexpectedly with a segmentation fault due to a race condition if the user selected a file that was already deleted but was still displayed in the window. This has been fixed and Nautilus does not terminate unexpectedly any longer.

BZ#654091

Previously, the GNOME Configuration (GConf) schemas were missing. As a consequence, the position and size of the folder windows were lost once the user closed the window. The missing GConf schemas have been added and the position and size of the folder windows are now saved and restored correctly.

BZ#661589

Prior to this update, Nautilus did not reflect the changes made to the locations of the XDG (Base Directory Specification) file system directories and used the old locations instead. As a consequence, files created on the desktop may have disappeared if the user logged on used a different user interface language. This problem has been fixed: the desktop is now refreshed with every change of the XDG directories.

BZ#666086

Previously, Nautilus could have become suspended when the user copied files from an FTP server. This was caused by an error in the GVFS (GNOME virtual file system) client dbus code which prevented recursive synchronous calls. This has been fixed and Nautilus no longer becomes suspended during the file transfers.

BZ#690147

Prior to this update, Nautilus did not refresh the folder buttons in the path bar when deleting the linked directories. When clicking on the folder icon in the path bar, an error message appeared. Now, folder buttons in the path bar are automatically removed when deleting the linked directory.

All users of nautilus are advised to upgrade to these updated packages, which fix these bugs.

4.187. NAUTILUS-OPEN-TERMINAL

4.187.1. RHBA-2011:1205 — nautilus-open-terminal bug fix update

An updated nautilus-open-terminal package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The nautilus-open-terminal extension provides the right-click "Open Terminal" option for Nautilus.

This updated nautilus-open-terminal package includes fixes for the following bugs:

BZ#630236

This update adds the untranslated string which was missing in the Japanese translation of the graphical user interface.

BZ#640496

Previously, the terminal failed to start if the user used a shell other than bash. The problem was caused by incorrect invocation parameters, which have been fixed and the terminal now launches properly.

BZ#716398

Previously, nothing happened if there was no terminal application installed and the user right-clicked on the desktop and selected "Open Terminal". With this update, the gnome-terminal package has been set as a hard dependency to guarantee at least one terminal application is available.

All users of nautilus-open-terminal are advised to upgrade to this updated package, which resolves these bugs.

4.188. NCOMPRESS

4.188.1. RHBA-2012:0043 — ncompress bug fix update

An updated ncompress package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The ncompress package contains the compress and uncompress file compression and decompression utilities, which are compatible with the original UNIX compress utility (.Z file extensions).

Bug Fix

BZ#781973

The ncompress utility previously relied on the glibc implementation of the memcpy() function. A recent glibc update optimized memcpy(), which resulted in data corruption in ncompress file compression and decompression. This update replaces memcpy() with the memmove() function and ncompress now works as expected.

All users of ncompress are advised to upgrade to this updated package, which fixes this bug.

4.189. NET-SNMP

4.189.1. RHBA-2011:1524 — net-snmp bug fix update

Updated net-snmp packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The net-snmp packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an SNMP library, an extensible agent, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the **`netstat`** command which uses SNMP, and a Tk/Perl management information base (MIB) browser.

Bug Fixes

BZ#678314

The previous version of **snmptrapd**, the Net-SNMP daemon for processing traps, leaked memory when processing incoming SNMP traps in embedded Perl. This caused the amount of consumed memory to grow over time, making the memory consumption even larger if the daemon was processing SNMPv1 traps. With this update, the underlying source code has been adapted to prevent such memory leaks, and processing incoming SNMP traps in embedded Perl no longer increases the memory consumption.

BZ#681949

On 64-bit systems, the previous version of **snmpd**, the Net-SNMP agent, gathered the disk IO and CPU usage statistics for **UCD-SNMP::systemStats** as 64-bit. However, relevant MIB describes these statistics as 32-bit and as a consequence, **snmpd** wrote the following message to the system log when processing the 64-bit values:

```
truncating integer value > 32 bits
```

This update adapts **snmpd** to collect values for **UCD-SNMP::systemStats** as 32-bit integers so that it no longer reports the aforementioned message to syslog.

BZ#683563

The previous version of the **snmpd** daemon did not detect errors when accessing the **/proc** file system. Consequent to this, an attempt to read information about an exited process while gathering information for a **HOST-RESOURCES-MIB::hrSWRunTable** table caused the daemon to terminate unexpectedly with a segmentation fault. This update adapts the underlying source code to make sure that such errors are now properly detected, and **snmpd** no longer crashes when populating **HOST-RESOURCES-MIB::hrSWRunTable**.

BZ#683680

Prior to this update, the **snmpd** daemon reported **HOST-RESOURCES-MIB::hrSystemDate** with an incorrect sign in the timezone offset. This update applies a patch to make sure the timezone offset is properly recalculated and the value reported by **snmpd** is now correct.

BZ#702165

Previously, the **snmpd** daemon tracked all network interfaces that were present on the system while it was running, including interfaces that were removed from the system during this time. Consequent to this, when an interface which had been removed was re-instantiated with the same name but with a different interface index, **snmpd** reported both interfaces separately in **IF-MIB::ifTable**. This typically happened to Point-to-Point Protocol (PPP) interfaces. This update adds two new options, **interface_fadeout** and **interface_replace_old**, to the **/etc/snmpd/snmpd.conf** configuration file, which allows system administrators to control the behavior of **snmpd** when two interfaces with the same name but a different interface index are detected. Refer to the **snmpd.conf**(5) manual page for details.

BZ#702171

When running on a system with two network interfaces with the same IP address, the previous version of the **snmpd** daemon silently ignored the second interface while populating **IP-MIB::ipAddressTable**. With this update, **snmpd** has been adapted to add a message that the second interface is being ignored to the system log in this scenario. This allows system administrators to determine why the second interface is missing from **IP-MIB::ipAddressTable**.

BZ#703682

The previous version of the **snmpd** daemon ignored **SIGCHLD** signals from processes that were spawned as a result of the **pass_persist** configuration option. However, this led to unnecessary defunct processes on the system. With this update, the **snmpd** daemon has been adapted to correctly process the **SIGCHLD** signals so that such defunct processes are no longer created.

BZ#707912

Prior this update, the **snmpd** daemon incorrectly ignored XFS file systems when populating **HOST-RESOURCES-MIB::hrFSTable**. This update adds support for the XFS file system to **HOST-RESOURCES-MIB::hrFSTable** so that **snmpd** no longer omits such file systems from the report.

BZ#708370

In previous versions of net-snmp, the **snmpd** daemon did not distinguish between outgoing SMUX messages and always incremented their **Request-ID**, even when multiple SMUX messages were sent as a result of one incoming SNMP request with multiple variables. However, *RFC 1227* requires that such SMUX messages should have the same **Request-ID**. With this update, **snmpd** properly recognizes multiple outgoing SMUX messages that are the result of one incoming SNMP request and assigns them the same **Request-ID**.

BZ#708947

When the system ran out of memory while populating **IP-MIB::ipNetToPhysicalTable**, the previous version of the **snmpd** daemon did not properly recover and may have terminated unexpectedly as a consequence. This update adapts the underlying source code to detect that the system is running out of memory, and **snmpd** no longer crashes in this situation.

BZ#710667

Prior to this update, the **netsnmp** module for the **Python** programming language did not properly initialize an SNMP session with SNMPv3 authentication. Consequent to this, and attempt to use such a session caused Python to terminate unexpectedly with a segmentation fault. This update ensures that SNMP sessions with SNMPv3 authentication are now initialized properly and can be used in Python modules as expected.

BZ#711481

The previous version of the **netsnmp** Python module did not properly parse OID names that included an MIB name (such as **IF-MIB::ifTable**). With this update, the regular expression for parsing OID names has been corrected and the aforementioned Python module now parses such names properly.

BZ#720704

Previously, the **snmpd** daemon did not verify the result of reading from a network socket in the SMUX module. Consequent to this, **snmpd** may have been unable to close erroneous SMUX sessions, because it failed to detect some network errors. With this update, the **snmpd** daemon has been adapted to properly detect errors when reading from a SMUX socket so that it can now react to these errors properly.

BZ#729738

When an **AgentX** subagent was being disconnected from the **snmpd** daemon, the daemon did not properly detach all outstanding SNMP requests from the internal session object representing this agent. As a consequence, **snmpd** could terminate unexpectedly while processing these requests. With this update, the **snmpd** daemon ensures that outstanding SNMP requests do not point to an AgentX session that is closed.

BZ#725657

When a binary is built with the **RELRO** flag, the ELF sections are reordered to include internal data sections before program's data sections, and the Global Offset Table (GOT) address section of the resulting ELF file is mapped read-only. This ensures that any attempt to overwrite the GOT entry and gain control over the execution flow of a program fails with an error. For this reason, the Net-SNMP daemons, binaries, and shared libraries are now built with full **RELRO** protection.

All users of net-snmp are advised to upgrade to these updated packages, which fix these bugs.

4.189.2. RHBA-2011:1839 — net-snmp bug fix update

Updated net-snmp packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The net-snmp packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an SNMP library, an extensible agent, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl Management Information Base (MIB) browser.

Bug Fix

BZ#753766

The SNMP daemon (snmpd) did not properly fill a set of watched socket file descriptors. Therefore, the daemon sometimes terminated unexpectedly with the "select: bad file descriptor" error message when more than 32 AgentX subagents connected to snmpd on 32-bit platforms or more than 64 subagents on 64-bit platforms. With this update, snmpd properly clears sets of watched file descriptors and thus it no longer crashes when handling a large number of subagents.

All users of net-snmp are advised to upgrade to these updated packages, which fix this bug.

4.189.3. RHBA-2013:1215 — net-snmp bug fix update

Updated net-snmp packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The net-snmp packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an SNMP library, an extensible agent, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl Management Information Base (MIB) browser.

Bug Fix

BZ#1002858

When an AgentX subagent disconnected from the SNMP daemon (snmpd), the daemon did not properly check that there were no active requests queued in the subagent and destroyed the session. Consequently, the session was referenced by snmpd later when processing queued requests and because it was already destroyed, snmpd terminated unexpectedly with a segmentation fault or looped indefinitely. This update adds several checks to prevent the destruction of sessions with active requests, and snmpd no longer crashes in the described scenario.

Users of net-snmp are advised to upgrade to these updated packages, which fix this bug.

4.189.4. RHBA-2013:0819 — net-snmp bug fix update

Updated net-snmp packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The net-snmp packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an SNMP library, an extensible agent, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl Management Information Base (MIB) browser.

Bug Fix

BZ#956287

Previously, snmpd erroneously checked the length of "SNMP-TARGET-MIB::snmpTargetAddrRowStatus" value in incoming "SNMP-SET" requests on 64-bit platforms. Consequently, snmpd sent an incorrect reply to the "SNMP-SET" request. With this update, the check of "SNMP-TARGET-MIB::snmpTargetAddrRowStatus" is fixed and it is possible to set it remotely using "SNMP-SET" messages.

Users of net-snmp are advised to upgrade to these updated packages, which fix this bug.

4.189.5. RHBA-2013:1110 — net-snmp bug fix update

Updated net-snmp packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The net-snmp packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an SNMP library, an extensible agent, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl Management Information Base (MIB) browser.

Bug Fix

BZ#986191

In previous Net-SNMP releases, snmpd reported an invalid speed of network interfaces in IF-MIB::ifTable and IF-MIB::ifXTable if the interface had a speed other than 10, 100, 1000 or 2500 MB/s. Thus, the net-snmp ifHighSpeed value returned was "0" compared to the correct speed as reported in ethtool, if the Virtual Connect speed was set to, for example, 0.9 Gb/s. With this update, the ifHighSpeed value returns the correct speed as reported in ethtool, and snmpd correctly reports non-standard network interface speeds.

Users of net-snmp are advised to upgrade to these updated packages, which fix this bug.

4.190. NET-TOOLS

4.190.1. RHBA-2011:1596 — net-tools bug fix update

An updated net-tools package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The net-tools package contains basic networking tools, including ifconfig, netstat, route, and others.

Bug Fixes

BZ#705110

Prior to this update, the "hostname -i" command failed to display related network addresses when the hostname was not included in the /etc/hosts file. The "hostname -f" command had the same issue with Fully Qualified Domain Names (FQDNs). To fix this issue, new "--all-fqdns" (or "-A") and "--all-ip-addresses" (or "-I") options have been implemented for the hostname command. These options are independent on the /etc/hosts content. The "hostname -I" command now displays all network addresses for all configured network interfaces, and the "hostname -A" command displays all FQDNs for all configured network interfaces of the host.

BZ#725348

The "netstat -p" command output incorrectly displayed a number in the PID/Program name column instead of the program name. The code has been modified to fix this issue, and netstat now shows the correct program name in this column.

BZ#732984

The netstat utility truncated IPv6 UDP sockets when the "--notrim" (or "-T") option was specified. This update fixes the issue, and whole IPv6 addresses are now displayed for UDP sockets when using netstat with this option.

BZ#680837

The route(8) manual page now includes an explicit description of the "mss M" option.

BZ#694766

The SYNOPSIS section of the plipconfig(8) manual page and the usage output of the plipconfig command have been modified to show correct plipconfig options.

All users of net-tools are advised to upgrade to this updated package, which resolves these issues.

4.190.2. RHBA-2012:0555 — net-tools bug fix update

Updated net-tools packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The net-tools packages contain basic networking tools. including hostname, ifconfig, netstat, or route.

Bug Fix

BZ#816375

Running the "hostname" command with the "-A, --all-fqdns" or "-I, --all-ip-addresses" option to display all Fully Qualified Domain Names (FQDNs) or network addresses of the host failed with the "Hostname lookup failure" error if the machine's host name was not resolved in DNS. With this update, these options are no longer dependent on name resolution; all FQDNs and network addresses of the host are now displayed as expected even if the host name cannot be resolved or is not included in the /etc/hosts file.

All users of net-tools are advised to upgrade to these updated packages, which fix this bug.

4.191. NETCF

4.191.1. RHBA-2011:1631 — netcf bug fix and enhancement update

Updated netcf packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The netcf packages contain a library for modifying the network configuration of a system. Network configuration is expressed in a platform-independent XML format, which netcf translates into changes to the system's "native" network configuration files.

The netcf packages have been upgraded to upstream version 0.1.9, which provides a number of bug fixes and enhancements over the previous version.

Bug Fix

BZ#713286

Prior to this update, certain interfaces associated configuration files in the /etc/sysconfig/network-scripts/ directory, but no corresponding device in the kernel. As a result, netcf returned an error status every time it was asked for the current status of an interface it was unable to find in the kernel, so management applications collected a large number of error log messages. With this update, failures to find an interface in the kernel are now ignored.

Enhancements

BZ#616060

In this update, netcf has been modified to capture the stdout and stderr output of ifup and ifdown, and, in the case of an error, forward that information back to the management application, which used netcf to start or stop an interface. This makes it easier to troubleshoot problems.

BZ#708476

Changes made to a host's network configuration by netcf (via netcf's API, or the ncftool commands) immediately and permanently modify the host's configuration files (in /etc/sysconfig/network-scripts/ifcfg-*). With this update, new API/virsh commands have been added to enable saving the current state of network configuration before any changes are made, and easily reverting to that configuration if any problems are encountered.

All users are advised to updated to these updated packages, which fix these bugs and add these enhancements.

4.192. NETWORKMANAGER

4.192.1. RHBA-2012:1112 — NetworkManager bug fix update

Updated NetworkManager packages that fix a bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

NetworkManager is a system network service that manages network devices and connections, attempting to keep active network connectivity when available. It manages Ethernet, wireless, mobile broadband (WWAN), and PPPoE (Point-to-Point Protocol over Ethernet) devices, and provides VPN integration with a variety of different VPN services.

Bug Fix

BZ#822271

When an existing DHCP lease was renewed, NetworkManager did not recognize it as a change in

DHCP state and failed to run the dispatcher scripts. Consequently, hostnames were purged from DHCP records. With this update the code has been improved and NetworkManager now handles same-state transitions correctly. Now, hostnames are not purged from the DHCP server when a lease is renewed.

Users of NetworkManager are advised to upgrade to these updated packages, which fix this bug.

4.192.2. RHBA-2011:1632 — NetworkManager bug fix and enhancement update

Updated NetworkManager packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

NetworkManager is a system network service that manages network devices and connections, attempting to keep active network connectivity when available. It manages Ethernet, wireless, mobile broadband (WWAN), and PPPoE devices, and provides VPN integration with a variety of different VPN services.

Bug Fixes

BZ#660666

NetworkManager did not recognize IBM CTC (Channel-to-Channel) devices, which made it impossible to install Red Hat Enterprise Linux on IBM S/390 machines which used CTC devices. NetworkManager now detects these devices properly, with the result that Red Hat Enterprise Linux can be installed on such machines.

BZ#696585

When connecting to a WLAN, pressing the Enter key in NetworkManager's dialog box had no effect and the dialog box remained open. However, the WLAN connection could be established by clicking the Connect button with the mouse. This happened because the Connect button was not defined as default action on confirmation in the code. With this update, the Connect button was marked as default and NetworkManager now launches the WLAN connection under these circumstances.

BZ#696916

Due to a memory access error, the connection profile configured in NetworkManager was not stored if an IPv6 address and an IPv6 gateway were specified. The code has been modified to prevent this issue and connection profiles are now stored correctly.

BZ#706338

Due to a timing issue in the libnm-glib library, NetworkManager produced a D-Bus error when a network driver was unloaded from the kernel. This error message was only for informational purposes and therefore did not need to appear in syslog messages. The message has been suppressed in the libnm-glib code, and the error message no longer occurs in any of the system logs.

BZ#747066

NetworkManager did not specify the initial frequency of an ad hoc wireless network when the frequency was not set by the user. If the network frequency was not set when authenticating with wpa_supplicant using the nl80211 supplicant driver, the connection attempt failed. NetworkManager has been modified to set a frequency that is supported by used network device if it is not specified by the user. Users can now connect to ad hoc wireless networks without problems in the scenario described.

BZ#659685

The RHSA-2010-0616 security advisory for the dbus-glib library introduced changes restricting access to D-Bus properties. Therefore under certain circumstances, NetworkManager failed to display the login banner when a user connected to a VPN. NetworkManager has been modified to respect dbus-glib limitations, and the login banner is now displayed correctly.

BZ#743555

The implementation of the wpa_supplicant application has recently been changed to use the nl80211 supplicant driver instead the WEXT wireless extension. Both methods use a different approach to show the level of a wireless network signal. This difference was not reflected in NetworkManager's code, therefore the signal level was shown incorrectly. NetworkManager has been modified to handle this feature correctly when using nl80211, and the signal level is now displayed correctly.

Enhancements

BZ#590096

NetworkManager did not send the system hostname to a DHCP server unless it was explicitly configured with a configuration file. NetworkManager now sends the hostname to the DHCP server by default.

BZ#713283

Roaming in RSA token-enabled enterprise Wi-Fi networks did not work properly, which resulted in the wpa_supplicant component upgrade to version 0.7.3. This update required new features to be implemented in NetworkManager. NetworkManager now includes the background scanning feature for the wpa_supplicant component and uses the nl80211 supplicant driver when adding a supplicant interface.

All users of NetworkManager are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.193. NETWORKMANAGER-OPENSWAN

4.193.1. RHBA-2011:1771 — NetworkManager-openswan bug fix update

An updated NetworkManager-openswan package that fixes various bug is now available for Red Hat Enterprise Linux 6.

NetworkManager-openswan contains software for integrating the Openswan VPN software with NetworkManager and the GNOME desktop.

Bug Fixes

BZ#684809

When an openswan VPN is established, the NetworkManager applet did not display any notification (login banner) and the error message, "Error getting 'Banner'", was logged. With this update, NetworkManager now displays the connection establishment notification as a tooltip for the NetworkManager icon.

BZ#702323

Prior to this update, networkmanager-openswan did not provide an export feature. Due to this, it was not possible to save the configuration settings in a file. This update adds this feature and now it is possible to export configuration settings to a file.

BZ#705890

Prior to this update, NetworkManager could not properly track the status of an openswan VPN. Consequently, when an openswan VPN was disconnected, NetworkManager did not remove the VPN padlock icon. This update fixes this issue and now the VPN padlock icon is removed after an openswan VPN connection is terminated.

All users of NetworkManager-openswan are advised to upgrade to this updated package, which fixes these bugs.

4.194. NEWT

4.194.1. RHEA-2011:1207 — newt enhancement update

Updated newt packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

Newt is a programming library for color text mode, widget-based user interfaces. Newt can be used to add stacked windows, entry widgets, check boxes, radio buttons, labels, plain text fields, and so on, to text mode user interfaces.

Enhancement

BZ#707704

Prior to this update, it was not possible to set a color of individual labels, scrollbars, entries, textboxes, and scales. With this update, setting a color of the aforementioned GUI elements is now possible.

All users of newt are advised to upgrade to these updated packages, which add this enhancement.

4.195. NFS-UTILS

4.195.1. RHSA-2011:1534 — Low: nfs-utils security, bug fix, and enhancement update

Updated nfs-utils packages that fix two security issues, various bugs, and add one enhancement are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The nfs-utils package provides a daemon for the kernel Network File System (NFS) server, and related tools such as the mount.nfs, umount.nfs, and showmount programs.

Security Fixes

CVE-2011-2500

A flaw was found in the way nfs-utils performed IP based authentication of mount requests. In configurations where a directory was exported to a group of systems using a DNS wildcard or NIS (Network Information Service) netgroup, an attacker could possibly gain access to other directories exported to a specific host or subnet, bypassing intended access restrictions.

CVE-2011-1749

It was found that the mount.nfs tool did not handle certain errors correctly when updating the mtab (mounted file systems table) file. A local attacker could use this flaw to corrupt the mtab file.

Bug Fixes

BZ#702273

The function responsible for parsing the /proc/mounts file was not able to handle single quote characters (') in the path name of a mount point entry if the path name contained whitespaces. As a consequence, an NFS-exported file system with such a mount point could not be unmounted. The parsing routine has been modified to parse the entries in the /proc/mounts file properly. All NFS file systems can be now unmounted as expected.

BZ#744657

On an IPv6-ready network, an NFS share could be mounted on the same location twice if one mount failed over from IPv6 to IPv4. This update prevents the failover to IPv4 under such circumstances.

BZ#732673

Prior to this update, NFS IPv6 unmounting failed. This happened because the umount command failed to find the respective mount address in the /proc/mounts file as it was expecting the mount address to be in brackets; however, the mount command saves the addresses without brackets. With this update, the brackets are stripped during the unmount process and the unmount process succeeds.

BZ#723780

Prior to this update, the system returned a misleading error message when an NFS mount failed due to TCP Wrappers constrictions on the server. With this update, the system returns the "mount.nfs: access denied by server while mounting" error message.

BZ#723438

The showmount command caused the rpc.mountd daemon to terminate unexpectedly with a segmentation fault. This happened because showmount requested a list of clients that have performed an NFS mount recently from the mount link list with an RPC (Remote Procedure Call) message sent to the daemon. However, the mount link list was not initialized correctly. With this update, the mount link list is initialized correctly and the problem no longer occurs.

BZ#731693

Mounting failed if no NFS version ("nfsvers") was defined. Also, the system returned no error message when the NFS version was specified incorrectly. With this update, the system returns the following error in such cases: "mount.nfs: invalid mount option was specified."

BZ#726112

The "showmount -e" command returned only the first client that imported a directory. This occurred due to an incorrect filtering of group names of clients. This bug has been fixed and the command returns all hosts, which import the directory.

BZ#697359

The nfs-utils manual pages did not contain description of the "-n" command-line option. This update adds the information to the rpc.svcgssd(8) man page.

BZ#720479

Due to an incorrect library order at link time, building nfs-utils from the source package resulted in a non-functional rpc.svcgssd daemon. This update reorders libgssglue in the spec file and the daemon works as expected in this scenario.

BZ#747400

Prior to this update, the rpcdebug tool run with the "pnfs" flag failed over to "nfs". This update adds the pNFS and FSCache debugging option and the problem no longer occurs.

BZ#729001

The debuginfo file for the rpcdebug binary was missing in the debuginfo package because the spec file defined the installation of the rpcdebug tool with the "-s" parameter. The parameter caused the binary to be stripped of debugging information on installation. With this update, the spec file was modified and the debuginfo file is now available in the debuginfo package.

BZ#692702

The rpc.idmapd daemon occasionally failed to start because the /var/lib/nfs/rpc_pipefs/ directory was not mounted on the daemon startup. With this update, the startup script checks if the directory is mounted.

Enhancement

BZ#715078

This update adds details about exports to specific IPv6 addresses or subnets to the exports(5) manual page.

Users of nfs-utils are advised to upgrade to these updated packages, which contain backported patches to resolve these issues and add this enhancement. After installing this update, the nfs service will be restarted automatically.

4.195.2. RHBA-2012:0673 — nfs-utils bug fix update

Updated nfs-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The nfs-utils packages provide a daemon for the kernel Network File System (NFS) server and related tools, which provides better performance than the traditional Linux NFS server used by most users. These packages also contain the mount.nfs, umount.nfs, and showmount programs.

Bug Fix

BZ#812450

Previously, the nfsd daemon was started before the mountd daemon. However, nfsd uses mountd to validate file handles. Therefore, if an existing NFS client sent requests to the NFS server when nfsd was started, the client received the ESTALE error causing client applications to fail. This update changes the startup order of the daemons: the mountd daemon is now started first so that it can be correctly used by nfsd, and the client no longer receives the ESTALE error in this scenario.

All users of nfs-utils are advised to upgrade to these updated packages, which fix this bug.

4.196. NFS-UTILS-LIB

4.196.1. RHBA-2011:1750 — nfs-utils-lib bug fix update

Updated nfs-utils-lib packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The nfs-utils-lib packages contain support libraries required by programs in the nfs-utils package.

Bug Fix

BZ#711210

Prior to this update, libnfsidmap did not support ldap. With this update, nfs-utils-lib provides ldap support.

All users of nfs-utils-lib are advised to upgrade to these updated packages, which fix this bug.

4.197. NMAP

4.197.1. RHBA-2011:0967 — nmap bug fix update

An updated nmap package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The nmap package provides a network exploration utility and a security scanner.

Bug Fix

BZ#621045

Prior to this update, the output of the "nmap -h" (or "nmap --help") command did not describe all the available nmap options that begin with the "-s" or "-P" prefix. As a result, a user could have been unable to research what options can be used to perform specific tasks with nmap. With this update, the bug has been fixed so that the output of "nmap -h" now describes all the aforementioned nmap options that were previously missing from the output.

All users of nmap are advised to upgrade to this updated package, which fixes this bug.

4.198. NSPR, NSS, NSS-SOFTOKN, AND NSS-UTIL

4.198.1. RHBA-2011:1584 — nspr, nss, nss-softokn, and nss-util bug fix and enhancement update

Updated nspr and nss related packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing, calendar time, basic memory management (the malloc() and free() functions), and shared library linking.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSLv2, SSLv3, TLS, and other security standards.

The nss component has been upgraded to upstream version 3.12.10, which provides a number of bug fixes and enhancements. (BZ#712958)

The nss-util package has been upgraded to upstream version 3.12.10, which provides a number of bug fixes and enhancements.(BZ#712960)

The nspr component has been upgraded to upstream version 4.8.8, which provides a number of bug fixes and enhancements. (BZ#712963)

Bug Fixes

BZ#668882

The CMS message decoder lost the pointer to enveloped data when decoding a message encoded with CMS (Cryptographic Message Syntax) that contained enveloped data. Consequently, the decoder got into an infinite loop and decoding terminated due to a stack overflow. With this update, the underlying code has been modified and the problem no longer occurs.

BZ#671266

The CMS routines failed to verify signed data when the SignerInfo object was using a subjectKeyID extension to indicate the signer and returned the following output:

```
signer 0 status = SigningCertNotFound cmsutil: problem decoding:
Unrecognized Object Identifier.
```

With this update, the subjectKeyID entries have been added to a temporary in-memory map of subjectKeyID values of certificates and the verification of such data now succeeds.

BZ#695018

When running debug builds, the pem module occasionally terminated with a segmentation fault when attempting to write to its log file due to insufficient permissions. This happened when the module was initially used by an application with superuser privileges, which created the log file, and subsequently by an application with non-superuser privileges as the application could not access the logging file due to lower privileges.

BZ#703658

When using the generateCRMFRequest tool to produce an RSA key larger than 2048, the process failed. This occurred because the crmf library used by generateCRMFRequest had the value for the maximum size for wrapped private keys (the MAX_WRAPPED_KEY_LEN property) hardcoded to 2048 bytes. The size is now adjusted based on the provided key attributes and the problem no longer occurs.

BZ#710298

On a 64-bit CPU with native AES instruction support, the intel_aes_decrypt_cbc_256() function did not work correctly when input and output buffers were the same and the function call failed with the message "data mismatch". This update fixes the code and the same buffer can be used for input and output.

BZ#747053

The health tests for deterministic random bit generator (DRBG) have been updated to better meet FIPS requirements.

BZ#747387

On NSS initialization, the module loader incorrectly initialized the PKCS#11 module even if the module was not adding any persistent certificate or module databases. Consequently, an attempt to synchronize usernames and passwords on an IPA server with data on an Active Directory server failed with the error "{'desc': "Can't contact LDAP server"}". The NSS module loader now checks the relevant flags and the problem no longer occurs.

Enhancements

BZ#688423

NSS supports pluggable ECC (Error-Correcting Code) memory.

BZ#724001, BZ#724002, BZ#724003, BZ#724004

The nss-softokn, nss-util, nss, and nspr libraries have been built with partial RELRO support (-Wl,-z,relro).

Users are advised to upgrade to these updated nspr and nss related packages, which fix the bugs and add the enhancements.

4.199. NSS

4.199.1. RHBA-2011:1838 — nss bug fix update

Updated nss packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

Bug Fix

BZ#766056

Recent changes to NSS re-introduced a problem where applications could not use multiple SSL client certificates in the same process. Therefore, any attempt to run commands that worked with multiple SSL client certificates, such as the "yum repolist" command, resulted in a re-negotiation handshake failure. With this update, a revised patch correcting this problem has been applied to NSS, and using multiple SSL client certificates in the same process is now possible again.

All users of nss are advised to upgrade to these updated packages, which fix this bug.

4.200. NSS-PAM-LDAPD

4.200.1. RHBA-2011:1705 — nss-pam-ldapd bug fix and enhancement update

An updated nss-pam-ldapd package that fixes multiple bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

[Updated 24 January 2012] This advisory has been updated with the correct package description in the Details section. The package included in this revised update has not been changed in any way from the package included in the original advisory.

The nss-pam-ldapd package provides the nss-pam-ldapd daemon (nslcd) which uses a directory server to look up name service information on behalf of a lightweight nsswitch module.

Bug Fixes

BZ#706454

When the nss-pam-ldapd package was installed, settings for the nslcd daemon were migrated from the configuration files used by the pam_ldap module or a previously-installed copy of the nss_ldap package. If the nslcd configuration file was modified, settings would be migrated again, often with an error. With this update, the migration is performed only if the package has not been previously installed.

BZ#706860

Prior to this update, when the nslcd daemon retrieved information about a user or group, the name of the user or group would be checked against the value of the "validnames" configuration setting. The default value of the setting expected the names to be at least three characters long, therefore names which were only two characters long were flagged as invalid. This could have negative impact on some installations. With this update, the default value of the "validnames" setting is modified to a minimum of two characters so that short names are accepted.

BZ#716822, BZ#720230

Due to the buffer used for the group field of a user password entry being not big enough, the primary group ID of a user could not be parsed if it contained more than nine digits. As a consequence, the nslcd daemon could drop some of the digits. With this update, nslcd is modified to parse large user IDs properly.

BZ#741362

An incorrect use of the strtol() call could cause large user ID values to overflow on 32-bit architectures. New functions have been implemented with this update, so that large user IDs are parsed correctly.

Enhancement

BZ#730309

Previously, if "DNS" was specified as the value of the LDAP "uri" setting in the /etc/nslcd.conf file, the nslcd service would attempt to look up DNS SRV records for the LDAP server (in order to determine which directory server to contact) only in the local host's current DNS domain. As a consequence, nslcd could not search for an LDAP server in a different domain. With this update, the DNS domain which is used in the lookup can now be specified by providing a value in the form "DNS:domainname".

All users of nss-pam-ldapd are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.200.2. RHBA-2012:0055 — nss-pam-ldapd bug fix update

An updated nss-pam-ldapd package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The nss-pam-ldapd provides the nss-pam-ldapd daemon (nslcd) which uses a directory server to look up name service information on behalf of a lightweight nsswitch module.

Bug Fix

BZ#771322

Previously, the nslcd daemon performed the idle time expiration check for the LDAP connection

before starting an LDAP search operation. On a lossy network or if the LDAP server was under a heavy load, a connection could time out after a successful check and the search operation then failed. With this update, the idle time expiration test is now performed during the LDAP search operation so that the connection now no longer expires under these circumstances.

All users of nss-pam-ldapd are advised to upgrade to this updated package, which fixes this bug.

4.201. NSS_DB

4.201.1. RHBA-2012:0346 — nss_db bug fix update

An updated nss_db package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The nss_db package contains a set of C library extensions, such as the Name Service Switch (nsswitch) module, which allow Berkeley Databases to be used as a primary source of aliases, groups, hosts, networks, protocols, users, services, or shadow passwords instead of, or in addition to, using flat files or the Network Information Service (NIS).

Bug Fix

BZ#788668

The previous update of nss_db attempted to fix a bug, which under certain circumstances prevented multi-threaded applications from obtaining complete lists of user's supplemental group memberships. This problem was not completely fixed due to an internal error that occurred when using an insufficiently large temporary buffer to parse a group entry with a large list of users. This update resolves the issue by resetting the buffer's contents after the buffer has been resized. Large group lists are thus correctly parsed and the entire list of user's supplemental groups is now correctly listed in this scenario.

All users of nss_db are advised to upgrade to this updated package, which fixes this bug.

4.202. OMPING

4.202.1. RHEA-2011:1576 — omping bug fix and enhancement update

An updated omping package that fixes several bugs and adds various enhancements is now available as a Technology Preview for Red Hat Enterprise Linux 6.

Open Multicast Ping (omping) is a tool for testing IP multicast functionality, primarily on a LAN (local area network). It allows users to test multicast and receive sufficient information to detect whether a potential problem exists in the network configuration, or lies elsewhere, as might be the case with a bug.

The omping package has been upgraded to upstream version 0.0.4, which provides a number of bug fixes and the following enhancements:

- support for Source Specific Multicast (SSM);
- support for broadcast;
- single node mode, which allows users to detect a misconfigured local firewall;
- more precise and rich statistics;

- rate limiting;
- duplicate packet detection.

BZ#696747

Users are advised to upgrade to this updated omping package, which resolves these bugs and adds these enhancements. Note that this package is included as a Technology Preview.

4.203. OPENCRYPTOKI

4.203.1. RHBA-2011:1572 — opencryptoki bug fix and enhancement update

Updated opencryptoki packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The openCryptoki package contains version 2.11 of the PKCS#11 API, implemented for IBM Cryptocards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded), the IBM eServer Cryptographic Accelerator (FC 4960 on IBM eServer System p), the IBM Crypto Express2 (FC 0863 or FC 0870 on IBM System z), and the IBM CP Assist for Cryptographic Function (FC 3863 on IBM System z).

Bug Fixes

BZ#734489

When setting the length of an RSA key for the IBM Cryptographic Accelerator (ICA) token, initialization of the CKA_MODULUS_BITS internal attribute of PKCS#11 was not properly tested and the RSA key length could have been set incorrectly. As a consequence, RSA key verification in the ICA token failed. To ensure that the RSA key is set correctly, two conditions have been added in the respective function in the ICA specific library. The RSA key operations now work properly on the ICA token.

BZ#730903

Prior to this update, the documentation provided with opencryptoki packages stated that users using opencryptoki needed to be members of the "pkcs11" group but did not mention the real privileges granted by adding a user to the group. Consequently, it was not clear that the members of the "pkcs11" group are assumed to be fully trusted. With this update opencryptoki(7) man page now contains a security note.

BZ#732756

Prior to this update, an unnecessary check in the attach_shared_memory() function was made which therefore required explicit group membership regardless of the current effective privileges. Consequently, upon installation of the opencryptoki packages and creation of the "pkcs11" group, the root user was added to the group. However, root user should not need access to the group to be able to access shared memory. With this update the shared memory checks have been corrected and root user no longer requires membership of the "pkcs11" group.

Enhancement

BZ#693779

The openCryptoki package has been upgraded to upstream version 2.4, which provides a number of bug fixes and enhancements over the previous version.

Users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.204. OPENLDAP

4.204.1. RHBA-2011:1514 — openldap bug fix and enhancement update

Updated openldap packages that fix number of bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

Bug Fixes

BZ#717738

In a utility which uses both OpenLDAP and Mozilla NSS (Network Security Services) libraries, OpenLDAP validates TLS peer and the certificate is cached by Mozilla NSS library. The utility then sometimes terminated unexpectedly on the **`NSS_Shutdown()`** function call because the client certificate was not freed and the cache could not be destroyed. With this update, the peer certificate is freed in OpenLDAP library after certificate validation is finished, all cache entries can now be deleted properly, and the **`NSS_Shutdown()`** call now succeeds as expected.

BZ#726984

When a program used the OpenLDAP library to securely connect to an LDAP server using SSL/TLS, while the server was using a certificate with a wildcarded common name (for example **`CN=*.example.com`**), the connection to the server failed. With this update, the library has been fixed to verify wildcard hostnames used in certificates correctly, and the connection to the server now succeeds if the wildcard common name matches the server name.

BZ#727533

Previously, if an OpenLDAP server was installed with an SQL back end, the server terminated unexpectedly after a few operations. An upstream patch, which updates data types for storing the length of the values by using the ODBC (Open Database Connectivity) interface, has been provided to address this issue. Now, the server no longer crashes when the SQL back end is used.

BZ#684810

The **`slapd-config(5)`** and **`ldap.conf(5)`** manual pages contained incorrect information about TLS settings. This update adds new TLS documentation relevant for the Mozilla NSS cryptographic library.

BZ#698921

When an LDIF (LDAP Data Interchange Format) input file was passed to the ldapadd utility or another **`openldap`** client tool, and the file was not terminated by a newline character, the client terminated unexpectedly. With this update, client utilities are able to properly handle such LDIF files, and the crashes no longer occur in the described scenario.

BZ#701227

When an LDIF (LDAP Data Interchange Format) input file was passed to the **ldapadd** utility or another **openldap** client tool, and a line in the file was split into two lines but was missing correct indentation (the second line has to be indented by one space character), the client terminated unexpectedly. With this update, client utilities are able to properly handle such filetype **LDIF** files, and the crashes no longer occur in the described scenario.

BZ#709407

When an OpenLDAP server was under heavy load or multiple replicating OpenLDAP servers were running, and, at the same time, TLS/SSL mode with certificates in PEM (Privacy Enhanced Mail) format was enabled, a race condition caused the server to terminate unexpectedly after a random amount of time (ranging from minutes to weeks). With this update, a mutex has been added to the code to protect calls of thread-unsafe Mozilla NSS functions dealing with PEM certificates, and the crashes no longer occur in the described scenario.

BZ#712358

When the openldap-servers package was installed on a machine while the initscript package was not already installed, some scriptlets terminated during installation and error messages were returned. With this update, initscripts have been defined as a required package for openldap-servers, and no error messages are now returned in the described scenario.

BZ#713525

When an openldap client had the **TLS_REQCERT** option set to **never** and the **TLS_CACERTDIR** option set to an empty directory, TLS connection attempts to a remote server failed as TLS could not be initialized on the client side. Now, **TLS_CACERTDIR** errors are ignored when **TLS_REQCERT** is set to **never**, thus fixing this bug.

BZ#722923

When a **slapd.conf** file was converted into a new **slapd.d** directory while the constraint overlay was in place, the **constraint_attribute** option of the **size** or **count** type was converted to the **olcConstraintAttribute** option with its value part missing. A patch has been provided to address this issue and constraint_attribute options are now converted correctly in the described scenario.

BZ#722959

When an openldap client had the **TLS_REQCERT** option set to **never** and the remote LDAP server uses a certificate issued by a CA (Certificate Authority) whose certificate has expired, connection attempts to the server failed due to the expired certificate. Now, expired CA certificates are ignored when **TLS_REQCERT** is set to **never**, thus fixing this bug.

BZ#723487

Previously, the openldap package compilation log file contained warning messages returned by strict-aliasing rules. These warnings indicated that unexpected runtime behavior could occur. With this update, the **-fno-strict-aliasing** option is passed to the compiler to avoid optimizations that can produce invalid code, and no warning messages are now returned during the package compilation.

BZ#723514

Previously, the **olcDDStolerance** option was shortening TTL (time to live) for dynamic entries, instead of prolonging it. Consequently, when an OpenLDAP server was configured with the dds overlay and the **olcDDStolerance** option was enabled, the dynamic entries were deleted before

their TTL expired. A patch has been provided to address this issue and the real lifetime of a dynamic entry is now calculated properly, as described in documentation.

BZ#729087

When a utility used the OpenLDAP library and TLS to connect to a server, while the library failed to verify a certificate or a key, a memory leak occurred in the **`tlsm_find_and_verify_cert_key()`** function. Now, verified certificates and keys are properly disposed of when their verification fails, and memory leaks no longer occur in the described scenario.

BZ#729095

When the **`olcVerifyClient`** option was set to **`allow`** in an OpenLDAP server or the **`TLS_REQCERT`** option was set to **`allow`** in a client utility, while the remote peer certificate was invalid, OpenLDAP server/client connection failed. With this update, invalid remote peer certificates are ignored, and connections can now be established in the described scenario.

BZ#731168

When multiple TLS operations were performed by clients or other replicated servers, with the openldap-servers package installed and TLS enabled, the server terminated unexpectedly. With this update, a mutex has been added to the code to protect calls of thread-unsafe Mozilla NSS initialization functions, and the crashes no longer occur in the described scenario.

BZ#732001

When the openldap-servers package was being installed on a server for the first time, redundant and confusing `/` character was printed during the installation. With this update, the responsible RPM scriptlet has been fixed and the `/` character is no longer printed in the described scenario.

BZ#723521

Previously, the **`slapo-unique`** manual page was missing information about quoting the keywords and URIs (uniform resource identifiers), and the attribute parameter was not described in the section about unique_strict configuration options. A patch has been provided to address these issues and the manual page is now up-to-date.

BZ#742592

Previously, when the openldap-servers package was installed, host-based ACLs did not work. With this update, configuration flags that enable TCP wrappers have been updated, and the host-based ACLs now work as expected.

Enhancements

BZ#730311

Previously, when a connection to an LDAP server was created by specifying search root DN (distinguished name) instead of the server hostname, the SRV records in DNS were requested and a list of LDAP server hostnames was generated. The servers were then queried in the order, in which the DNS server returned them but the priority and weight of the records were ignored. This update adds support for priority/weight of the DNS SRV records, and the servers are now queried according to their priority/weight, as required by RFC 2782.

BZ#712494

In the default installation of the openldap-servers package, the configuration database (**`cn=config`**) could only be modified manually when the **`slapd`** daemon was not running. With this update, the

`ldapi:///` interface has been enabled by default, and the ACLs (access control lists) now enable the root user to modify the server configuration without stopping the server and using OpenLDAP client tools if he is authenticated using **`ldapi:///`** and the SASL/EXTERNAL mechanism.

BZ#723999

The openldap package was compiled without RELRO (read-only relocations) flags and was therefore vulnerable to various attacks based on overwriting the ELF section of a program. To increase the security of the package, the openldap spec file has been modified to use the **`-Wl,-z,relro`** flags when compiling the package. The openldap package is now provided with partial RELRO protection.

Users of **openldap** are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.205. OPENMOTIF

4.205.1. RHBA-2011:1228 — openmotif bug fix update

An updated openmotif package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The openmotif package includes the Motif shared libraries needed to run applications that are dynamically linked against Motif, as well as the Motif Window Manager (MWM).

Bug Fix

BZ#584300

Previously, under certain circumstances, LabelGadget could have drawn over a parent window with the background color and, if using the Xft fonts, also over the text. With this update, the text and background drawing functionality has been fixed so that the aforementioned problems do not occur anymore.

All users of openmotif are advised to upgrade to this updated package, which fixes this bug.

4.206. OPENOFFICE.ORG

4.206.1. RHSA-2012:0705 — Important: openoffice.org security update

Updated openoffice.org packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

OpenOffice.org is an office productivity suite that includes desktop applications, such as a word processor, spreadsheet application, presentation manager, formula editor, and a drawing program.

Security Fixes

CVE-2012-2334

An integer overflow flaw, leading to a buffer overflow, was found in the way OpenOffice.org processed an invalid Escher graphics records length in Microsoft Office PowerPoint documents. An

attacker could provide a specially-crafted Microsoft Office PowerPoint document that, when opened, would cause OpenOffice.org to crash or, potentially, execute arbitrary code with the privileges of the user running OpenOffice.org.

CVE-2012-1149

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the JPEG, PNG, and BMP image file reader implementations in OpenOffice.org. An attacker could provide a specially-crafted JPEG, PNG, or BMP image file that, when opened in an OpenOffice.org application, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Upstream acknowledges Sven Jacobi as the original reporter of CVE-2012-2334, and Tielei Wang via Secunia SVCRP as the original reporter of CVE-2012-1149.

All OpenOffice.org users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of OpenOffice.org applications must be restarted for this update to take effect.

4.207. OPENSCAP

4.207.1. RHBA-2011:1618 — openscap bug fix and enhancement update

Updated openscap packages that fix various bugs and add several enhancements are now available for Red Hat Enterprise Linux 6.

The Security Content Automation Protocol (SCAP) is a line of standards that provide a standard language for the expression of Computer Network Defense (CND) related information. OpenSCAP is a set of open source libraries for the integration of SCAP.

The openscap packages have been upgraded to upstream version 0.8.0, which provides a number of bug fixes and enhancements over the previous version. The most important changes include support for Open Vulnerability and Assessment Language (OVAL) version 5.8. (BZ#697648)

All users of openscap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.208. OPENSSH

4.208.1. RHBA-2011:1551 — openssh bug fix and enhancement update

Updated openssh packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

OpenSSH is OpenBSD's Secure Shell (SSH) protocol implementation. These packages include the core files necessary for the OpenSSH client and server.

Bug Fixes

BZ#685060

Prior to this update, SELinux could prevent users from uploading new files to their home directories in a chrooted Secure File Transfer Protocol (SFTP) environment. This bug has been fixed and users are now able to upload and download files in chrooted environment using SFTP.

BZ#705397, BZ#728459

Prior to this update, multiple manual pages contained formatting errors. As a consequence, error messages or warnings could be displayed when viewing these manual pages. The formatting has been corrected and the error messages and warnings are no longer displayed.

BZ#708056

Previously, when the SSH_USE_STRONG_RNG environment variable was set to 1, openssh read 48 bytes from the /dev/random number generator to generate a seed. This seed was too long and caused long delays on ssh or sshd startup and when connections were received. Now, the SSH_USE_STRONG_RNG variable contains the number of bytes that should be pulled from /dev/random (with a minimum default value of six) and the delays no longer occur.

BZ#714554

Previously, when restarting the dovecot service, ssh could become unresponsive. With this update, the source code is modified and the dovecot service now restarts properly and without hanging.

BZ#729021

Prior to this update, the debuginfo file was missing in the debuginfo package. With this update, the debuginfo file is included in the package and users can now view all debug information.

BZ#731939

Previously, the lastlog command did not show the last login of a user with a big user ID on 32-bit architectures. With this update, the source code is modified so that the last login information is now always recorded.

Enhancement

BZ#695781

With this update, multiple manual pages now describe Internet Protocol version 6 (IPv6) usage.

All users of openssh are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.208.2. RHEA-2012:0065 — openssh enhancement update

Updated openssh packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

OpenSSH is OpenBSD's Secure Shell (SSH) protocol implementation. These packages include the core files necessary for the OpenSSH client and server.

Enhancement

BZ#782367

Previously, OpenSSH could use the Advanced Encryption Standard New Instructions (AES-NI) instruction set only with the AES Cipher-block chaining (CBC) cipher. This update adds support for Counter (CTR) mode encryption in OpenSSH so the AES-NI instruction set can now be used efficiently also with the AES CTR cipher.

All users of openssh are advised to upgrade to these updated packages, which add this enhancement.

4.209. OPENSSL

4.209.1. RHSA-2012:0059 — Moderate: openssl security update

Updated openssl packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

Security Fixes

CVE-2011-4108

It was discovered that the Datagram Transport Layer Security (DTLS) protocol implementation in OpenSSL leaked timing information when performing certain operations. A remote attacker could possibly use this flaw to retrieve plain text from the encrypted packets by using a DTLS server as a padding oracle.

CVE-2011-4576

An information leak flaw was found in the SSL 3.0 protocol implementation in OpenSSL. Incorrect initialization of SSL record padding bytes could cause an SSL client or server to send a limited amount of possibly sensitive data to its SSL peer via the encrypted connection.

CVE-2011-4577

A denial of service flaw was found in the RFC 3779 implementation in OpenSSL. A remote attacker could use this flaw to make an application using OpenSSL exit unexpectedly by providing a specially-crafted X.509 certificate that has malformed RFC 3779 extension data.

CVE-2011-4619

It was discovered that OpenSSL did not limit the number of TLS/SSL handshake restarts required to support Server Gated Cryptography. A remote attacker could use this flaw to make a TLS/SSL server using OpenSSL consume an excessive amount of CPU by continuously restarting the handshake.

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

4.209.2. RHSA-2012:0426 — Moderate: openssl security and bug fix update

Updated openssl packages that fix two security issues and one bug are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

Security Fixes

CVE-2012-1165

A NULL pointer dereference flaw was found in the way OpenSSL parsed Secure/Multipurpose Internet Mail Extensions (S/MIME) messages. An attacker could use this flaw to crash an application that uses OpenSSL to decrypt or verify S/MIME messages.

CVE-2012-0884

A flaw was found in the PKCS#7 and Cryptographic Message Syntax (CMS) implementations in OpenSSL. An attacker could possibly use this flaw to perform a Bleichenbacher attack to decrypt an encrypted CMS, PKCS#7, or S/MIME message by sending a large number of chosen ciphertext messages to a service using OpenSSL and measuring error response times.

This update also fixes a regression caused by the fix for CVE-2011-4619, released via RHSA-2012:0060 and RHSA-2012:0059, which caused Server Gated Cryptography (SGC) handshakes to fail.

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

4.209.3. RHSA-2012:0518 — Important: openssl security update

Updated openssl, openssl097a, and openssl098e packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

Security Fix

CVE-2012-2110

Multiple numeric conversion errors, leading to a buffer overflow, were found in the way OpenSSL parsed ASN.1 (Abstract Syntax Notation One) data from BIO (OpenSSL's I/O abstraction) inputs. Specially-crafted DER (Distinguished Encoding Rules) encoded data read from a file or other BIO input could cause an application using the OpenSSL library to crash or, potentially, execute arbitrary code.

All OpenSSL users should upgrade to these updated packages, which contain a backported patch to resolve this issue. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

4.209.4. RHSA-2012:0699 — Moderate: openssl security and bug fix update

Updated openssl packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

Security Fix

CVE-2012-2333

An integer underflow flaw, leading to a buffer over-read, was found in the way OpenSSL handled DTLS (Datagram Transport Layer Security) application data record lengths when using a block cipher in CBC (cipher-block chaining) mode. A malicious DTLS client or server could use this flaw to crash its DTLS connection peer.

Red Hat would like to thank the OpenSSL project for reporting this issue. Upstream acknowledges Codenomicon as the original reporter.

On Red Hat Enterprise Linux 6, this update also fixes an uninitialized variable use bug, introduced by the fix for CVE-2012-0884 (released via RHSA-2012:0426). This bug could possibly cause an attempt to create an encrypted message in the CMS (Cryptographic Message Syntax) format to fail.

All OpenSSL users should upgrade to these updated packages, which contain a backported patch to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

4.209.5. RHBA-2011:1730 — openssl bug fix and enhancement update

Updated openssl packages that fix two bugs and add several enhancements are now available for Red Hat Enterprise Linux 6.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library.

Bug Fixes

BZ#693863

Prior to this update, repeatedly loading and unloading the CHIL engine could cause the calling program to terminate unexpectedly with a segmentation fault. This happened, because a function pointer was not properly cleared after the engine was unloaded. With this update, the underlying source code has been corrected to clear the function pointer when the engine is unloaded, and the calling program no longer crashes in this scenario.

BZ#740188

Due to missing variable initialization, the CHIL engine could occasionally fail to load. This update corrects the underlying source code to properly initialize this variable so that the CHIL engine is no longer prevented from loading.

Enhancements

BZ#696389

The performance of the AES encryption algorithm on CPUs with the AES-NI instruction set, as well as SHA-1 and RC4 algorithms on 32-bit and 64-bit x86 architectures has been significantly improved.

BZ#708511

For testing purposes, the OpenSSL source RPM package can now be built without additional patches.

BZ#723994

Partial RELRO is now enabled during the build of the OpenSSL libraries to improve security vulnerability properties of applications that use these libraries.

BZ#726081

Users can now explicitly disable the built-in AES-NI (Advanced Encryption Standard New Instruction) CPU instruction acceleration support by setting the OPENSSL_DISABLE_AES_NI environment variable to any value.

BZ#740872

Prior to this update, there was no direct KAT (known answer test) self-test for the SHA-2 algorithms in FIPS mode; these algorithms were self-tested only during the HMAC self-tests. This update provides an implementation of the direct KAT self-test for SHA-2 algorithms.

BZ#693858

Previously, the manual and help pages for various subcommands of the openssl utility did not specify all digest algorithms. This update adapts these pages and users are now instructed to run the "openssl dgst -h" command, which lists all available digests.

All users of openssl are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.209.6. RHBA-2012:0360 — openssl bug fix update

An updated openssl package that fixes one bug is now available for Red Hat Enterprise Linux 6.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full strength general-purpose cryptography library.

Bug Fix

BZ#799256

The functions that implement Counter (CTR), Output Feedback (OFB), and Cipher Feedback (CFB) block cipher modes previously incorrectly reset the counter of the remaining bytes of a block that had not been used in the previous encryption or decryption operation. Consequently, calling the encryption function on a small amount of data, that was not aligned to the size of the block, led to incorrect data encryption or decryption in the aforementioned modes. An upstream patch has been applied to correct the underlying functions, and both encryption and decryption now work as expected in CTR, OFB, and CFB modes.

All users of openssl are advised to upgrade to this updated package, which fixes this bug.

4.210. OPENSSL-IBMCA

4.210.1. RHBA-2011:1568 — openssl-ibmca bug fix and enhancement update

An updated openssl-ibmca package that fixes several bugs and adds various enhancements is available for Red Hat Enterprise Linux 6.

The openssl-ibmca package provides a dynamic OpenSSL engine for the IBM eServer Cryptographic Accelerator (ICA) crypto hardware on IBM eServer zSeries machines.

The openssl-ibmca package has been upgraded to upstream version 1.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#694194)

All users of openssl-ibmca are advised to upgrade to this updated package, which fixes these bug and adds these enhancements.

4.210.2. RHBA-2012:0433 — openssl-ibmca bug fix update

An updated openssl-ibmca package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The openssl-ibmca package provides a dynamic OpenSSL engine for the IBM eServer Cryptographic Accelerator (ICA) crypto hardware on IBM eServer zSeries machines.

Bug Fix

BZ#804612

Due to a bug in the ibmca OpenSSL engine code, applications using the OpenSSL library terminated unexpectedly with a segmentation fault when running the ibmca engine with ciphers enabled in output feedback (OFB) mode on IBM System z, z196 series, hardware. A patch has been applied to address this issue, ensuring that the OpenSSL library no longer crashes under these circumstances.

All users of openssl-ibmca are advised to upgrade to this updated package, which fixes this bug.

4.211. OPENSWAN

4.211.1. RHBA-2011:1761 — openswan bug fix and enhancement update

An updated openswan package that fixes several bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

Openswan is a free implementation of IPsec (Internet Protocol Security) and IKE (Internet Key Exchange) for Linux. The openswan package contains the daemons and user space tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4306).

Bug Fixes

BZ#703473

Openswan did not handle protocol and port configuration correctly if the ports were defined and the host was defined with its hostname instead of its IP address. This update solves this issue, and Openswan now correctly sets up policies with the correct protocol and port under such circumstances.

BZ#703985

Prior to this update, very large security label strings received from a peer were being truncated. The truncated string was then still used. However, this truncated string could turn out to be a valid string, leading to an incorrect policy. Additionally, erroneous queuing of on-demand requests of setting up an

IPsec connection was discovered in the IKEv2 (Internet Key Exchange) code. Although not harmful, it was not the intended design. This update fixes both of these bugs and Openswan now handles the IKE setup correctly.

BZ#704548

Previously, Openswan failed to set up AH (Authentication Header) mode security associations (SAs). This was because Openswan was erroneously processing the AH mode as if it was the ESP (Encrypted Secure Payload) mode and was expecting an encryption key. This update fixes this bug and it is now possible to set up AH mode SAs properly.

BZ#711975

IPsec connections over a loopback interface did not work properly when a specific port was configured. This was because incomplete IPsec policies were being set up, leading to connection failures. This update fixes this bug and complete policies are now established correctly.

BZ#737975

Openswan failed to support retrieving Certificate Revocation Lists (CRLs) from HTTP or LDAP CRL Distribution Points (CDPs) because the flags for enabling CRL functionality were disabled on compilation. With this update, the flags have been enabled and the CRL functionality is available as expected.

BZ#737976

Openswan failed to discover some certificates. This happened because the README.x509 file contained incorrect information on the directories to be scanned for certification files and some directories failed to be scanned. With this update, the file has been modified to provide accurate information.

BZ#738385

The Network Manager padlock icon was not cleared after a VPN connection terminated unexpectedly. This update fixes the bug and the padlock icon is cleared when a VPN connection is terminated as expected.

BZ#742632

Openswan sent wrong IKEv2 (Internet Key Exchange) ICMP (Internet Control Message Protocol) selectors to an IPsec destination. This happened due to an incorrect conversion of the host to network byte order. This update fixes this bug and Openswan now sends correct ICMP selectors.

BZ#749605

The Pluto daemon terminated unexpectedly with a segmentation fault after an IP address had been removed from one end of an established IPsec tunnel. This occurred if the other end of the tunnel attempted to reuse the particular IP address to create a new tunnel as the previous tunnel failed to close properly. With this update, such tunnel is closed properly and the problem no longer occurs.

Enhancement

BZ#737973

On run, the "ipsec barf" and "ipsec verify" commands load new kernel modules, which influences the system configuration. This update adds the "iptable-save" command, which uses only iptables and does not load kernel modules.

Users are advised to upgrade to this updated openswan package, which fixes these bugs and adds the enhancement.

4.211.2. RHBA-2012:0339 — openswan bug fix update

An updated openswan package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Openswan supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4306).

Bug Fixes

BZ#786434

The Openswan IKEv2 implementation did not correctly process an IKE_SA_INIT message containing an INVALID_KE_PAYLOAD Notify Payload. With this fix, Openswan now sends the INVALID_KE_PAYLOAD notify message back to the peer so that IKE_SA_INIT can restart with the correct KE payload.

BZ#786435

Previously, Openswan sometimes generated a KE payload that was 1 byte shorter than specified by the Diffie-Hellman algorithm. Consequently, IKE renegotiation failed at random intervals. An error message in the following format was logged:

```
next payload type of ISAKMP Identification Payload has an unknown value
```

This update checks the length of the generated key and if it is shorter than required, leading zero bytes are added.

All users of openswan are advised to upgrade to this updated package, which fixes these bugs. Note that the NSS library package needs to be version 3.13 or later for the KE payload and IKE renegotiation issues to be fully resolved.

4.211.3. RHBA-2012:0541 — openswan bug fix update

Updated openswan packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

Openswan is a free implementation of IPsec (Internet Protocol Security) and IKE (Internet Key Exchange) for Linux. The openswan package contains the daemons and user space tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6 and later also supports IKEv2 (Internet Key Exchange Protocol Version 2), which is defined in RFC5996.

Bug Fixes

BZ#813192

Openswan incorrectly processed traffic selector messages proposed by the responder (the endpoint responding to an initiated exchange) if the traffic selectors were confined to a subset of the initially proposed traffic selectors. As consequence, Openswan set up CHILD security associations (SAs) incorrectly. With this update, Openswan initiates a new connection for the reduced set of traffic selectors, and sets up IKE CHILD SAs accordingly.

BZ#813194

Openswan incorrectly processed traffic selector messages proposed by the initiator (the endpoint which started an exchange) if the traffic selectors were confined to a subset of the initially proposed traffic selectors. As a consequence, Openswan set up CHILD SAs incorrectly. With this update, Openswan initiates a new connection for the reduced set of traffic selectors, and sets up IKE CHILD SAs accordingly.

BZ#813355

When processing an IKE_AUTH exchange and the RESERVED field of the IKE_AUTH request or response messages was modified, Openswan did not ignore the field as expected according to the IKEv2 RFC5996 specification. Consequently, the IKE_AUTH messages were processed as erroneous messages by Openswan and the IKE_AUTH exchange failed. With this update, Openswan has been modified to ignore reserved fields as expected and IKE_AUTH exchanges succeed in this scenario.

BZ#813356

When processing an IKE_SA_INIT exchange and the RESERVED field of the IKE_SA_INIT request or response messages was modified, Openswan did not ignore the field as expected according to the IKEv2 RFC5996 specification. Consequently, IKE_SA_INIT messages with reserved fields set were processed as erroneous messages by Openswan and the IKE_SA_INIT exchange failed. With this update, Openswan has been modified to ignore reserved fields as expected and IKE_SA_INIT exchanges succeed in this scenario.

BZ#813357

Previously, Openswan did not behave in accordance with the IKEv2 RFC5996 specification and ignored IKE_AUTH messages that contained an unrecognized Notify payload. This resulted in IKE SAs being set up successfully. With this update, Openswan processes any unrecognized Notify payload as an error and IKE SA setup fails as expected.

BZ#813360

When processing an INFORMATIONAL exchange, the responder previously did not send an INFORMATIONAL response message as expected in reaction to the INFORMATIONAL request message sent by the initiator. As a consequence, the INFORMATIONAL exchange failed. This update corrects Openswan so that the responder now sends an INFORMATIONAL response message after every INFORMATIONAL request message received, and the INFORMATIONAL exchange succeeds as expected in this scenario.

BZ#813362

When processing an INFORMATIONAL exchange with a Delete payload, the responder previously did not send an INFORMATIONAL response message as expected in reaction to the INFORMATIONAL request message sent by the initiator. As a consequence, the INFORMATIONAL exchange failed and the initiator did not delete IKE SAs. This updates corrects Openswan so that the responder now sends an INFORMATIONAL response message and the initiator deletes IKE SAs as expected in this scenario.

BZ#813364

When the responder received an INFORMATIONAL request with a Delete payload for a CHILD SA, Openswan did not process the request correctly and did not send the INFORMATIONAL response message to the initiator as expected according to the RFC5996 specification. Consequently, the responder was not aware of the request and only the initiator's CHILD SA was deleted. With this update, Openswan sends the response message as expected and the CHILD SA is deleted properly on both endpoints.

BZ#813366

Previously, Openswan did not respond to INFORMATIONAL requests with no payloads that are used for dead-peer detection. Consequently, the initiator considered the responder to be a dead peer and deleted the respective IKE SAs. This update modifies Openswan so that an empty INFORMATIONAL response message is now sent to the initiator as expected, and the initiator no longer incorrectly deletes IKE SAs in this scenario.

BZ#813372

When processing an INFORMATIONAL exchange and the RESERVED field of the INFORMATIONAL request or response messages was modified, Openswan did not ignore the field as expected according to the IKEv2 RFC5996 specification. Consequently, the INFORMATIONAL messages were processed as erroneous by Openswan, and the INFORMATIONAL exchange failed. With this update, Openswan has been modified to ignore reserved fields as expected and INFORMATIONAL exchanges succeed in this scenario.

BZ#813378

When the initiator received an INFORMATIONAL request with a Delete payload for an IKE SA, Openswan did not process the request correctly and did not send the INFORMATIONAL response message to the responder as expected according to the RFC5996 specification. Consequently, the initiator was not aware of the request and only the responder's IKE SA was deleted. With this update, Openswan sends the response message as expected and the IKE SA is deleted properly on both endpoints.

BZ#813379

IKEv2 requires each IKE message to have a sequence number for matching a request and response when re-transmitting the message during the IKE exchange. Previously, Openswan incremented sequence numbers incorrectly so that IKE messages were processed in the wrong order. As a consequence, any messages sent by the responder were not processed correctly and any subsequent exchange failed. This update modifies Openswan to increment sequence numbers in accordance with the RFC5996 specification so that IKE messages are matched correctly and exchanges succeed as expected in this scenario.

BZ#813565

Openswan did not ignore the minor version number of the IKE_SA_INIT request messages as required by the RFC5996 specification. Consequently, if the minor version number of the request was higher than the minor version number of the IKE protocol used by the receiving peer, Openswan processed the IKE_SA_INIT messages as erroneous and the IKE_SA_INIT exchange failed. With this update, Openswan has been modified to ignore the Minor Version fields of the IKE_SA_INIT requests as expected and the IKE_SA_INIT exchange succeeds in this scenario.

BZ#814600

Older versions of kernel required the output length of the HMAC hash function to be truncated to 96 bits therefore Openswan previously worked with 96-bit truncation length when using the HMAC-SHA2-256 algorithm. However, newer kernels require the 128-bit HMAC truncation length, which is as per the RFC4868 specification. Consequently, this difference could cause incompatible SAs to be set on IKE endpoints due to one endpoint using 96-bit and the other 128-bit output length of the hash function. This update modifies the underlying code so that Openswan now complies with RFC4868 and adds support for the new kernel configuration parameter, sha2_truncbug. If the "sha2_truncbug" parameter is set to "yes", Openswan now passes the correct key length to the kernel, which ensures interoperability between older and newer kernels.

All users of openswan are advised to upgrade to these updated packages, which fix these bugs.

4.211.4. RHBA-2013:1160 — openswan bug fix update

Updated openswan packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks.

Bug Fix

BZ#983451

The openswan package for Internet Protocol Security (IPsec) contains two diagnostic commands, "ipsec barf" and "ipsec look", that can cause the iptables kernel modules for NAT and IP connection tracking to be loaded. On very busy systems, loading such kernel modules can result in severely degraded performance or lead to a crash when the kernel runs out of resources. With this update, the diagnostic commands do not cause loading of the NAT and IP connection tracking modules. This update does not affect systems that already use IP connection tracking or NAT as the iptables and ip6tables services will already have loaded these kernel modules.

Users of openswan are advised to upgrade to these updated packages, which fix this bug.

4.212. OPROFILE

4.212.1. RHBA-2011:1712 — oprofile bug fix and enhancement update

An updated oprofile package that fixes one bug and adds two enhancements is now available for Red Hat Enterprise Linux 6.

OProfile is a system-wide profiler for Linux systems. The profiling runs transparently in the background and profile data can be collected at any time. OProfile uses the hardware performance counters provided on many processors, and can use the Real Time Clock (RTC) for profiling on processors without counters.

Bug Fix

BZ#717860

Previously, OProfile could encounter a buffer overrun in the OProfile daemon. This update modifes oprofiled so that OProfile now checks and reports if the filename is too large for the buffer.

Enhancements

BZ#696565

Previously, the OProfile profiler did not provide the performance monitoring events for the Intel Sandy Bridge processor. This update provides the files for the Intel Sandy Bridge processor specific performance events and adds the code to identify Intel Sandy Bridge processors. Now, OProfile provides Intel Sandy Bridge specific events.

BZ#695851

Previously, the OProfile profiler did not identify some Intel Westmere processors causing OProfile to use the fallback Intel Architected events. Now, OProfile provides Intel Westmere specific events for Intel Westmere-EX processors (model 0x2f).

All OProfile users are advised to upgrade to this updated package which fixes this bug and adds these enhancements.

4.213. PACEMAKER

4.213.1. RHBA-2011:1669 — pacemaker bug fix and enhancement update

Updated pacemaker packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Pacemaker Cluster Resource Manager provides the ability to create and manage high-availability server applications in the event of system downtime.

The pacemaker packages have been upgraded to upstream version 1.1.6, which provides a number of bug fixes and enhancements over the previous version. In particular, this update fixes the following bugs:

BZ#708722

Prior to this update, when the pacemaker daemon did not have permission to write to the /var/log/cluster/corosync.log file, it wrote the following error to the system log:

```
attrd: Cannot append to /var/log/cluster/corosync.log: Permission denied
```

This update applies a patch to ensure that when such an error occurs, Pacemaker logs this problem on startup and no longer tries to access this file.

BZ#720136

When using the CRM command line interface, running the "configure", "template", and "list" commands in this particular order caused the crm process to terminate unexpectedly with the following error:

```
NameError: global name 'listconfigs' is not defined
```

With this update, the underlying source code has been modified to address this issue so that CRM no longer crashes.

BZ#743175

Under certain circumstances, an attempt to fence a node may have caused Pacemaker to stop responding when accessing the /var/run/cluster/fenced_override file. With this update, this error no longer occurs, and Pacemaker now works as expected in this scenario.

BZ#745526

Prior to this update, an error in the interaction between Pacemaker and CMAN's fencing subsystem prevented reliable fencing operation. This update applies a patch that corrects this error so that such fencing operations are now reliable.

BZ#708797

In the previous version of the crm(8) manual page, the EXAMPLES section incorrectly listed several example commands on a single line. This made it particularly difficult for a reader to distinguish these commands. This update introduces a new, completely rewritten manual page, which lists each example command on a separate line.

All users who want to use the pacemaker Technology Preview should upgrade to these updated packages, which provide numerous bug fixes and enhancements.

4.214. PAM

4.214.1. RHEA-2011:1732 — pam enhancement update

Updated pam packages that add one enhancement are now available for Red Hat Enterprise Linux.

Pluggable Authentication Modules (PAM) provide a system for administrators to set up authentication policies without the need to recompile programs to handle authentication.

Enhancement

BZ#727286

With this update, the libraries are recompiled with the partial read only relocation (RELRO) flag to enhance the security of applications that use the libraries.

All pam users are advised to upgrade to these updated packages, which add this enhancement.

4.214.2. RHEA-2012:0482 — pam enhancement update

Updated pam packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

Pluggable Authentication Modules (PAM) provide a system to set up authentication policies without the need to recompile programs to handle authentication.

Enhancement

BZ#809370

The pam_cracklib is a PAM module for password-quality checking used by various applications. With this update, the pam_cracklib module has been improved with additional password-quality checks. The pam_cracklib module now allows to check whether a new password contains the words from the GECOS field from entries in the "/etc/passwd" file. The GECOS field is used to store additional information about the user, such as the user's full name or a phone number, which could be used by an attacker for an attempt to crack the password. The pam_cracklib module now also allows to specify the maximum allowed number of consecutive characters of the same class (lowercase, uppercase, number and special characters) in a password.

All users of pam are advised to upgrade to these updated packages, which add this enhancement.

4.215. PAM_KRB5

4.215.1. RHBA-2011:1704 — pam_krb5 bug fix update

An updated pam_krb5 package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The pam_krb5 package allows PAM-aware applications to check user passwords with the help of a Kerberos KDC.

Bug Fixes

BZ#690832

When a client logged into a remote host using SSH with GSSAPI authentication, configured to re-delegate credentials when the client obtains fresh credentials, pam_krb5 created a new credential cache on the remote host in addition to the cache created by SSH. Consequently, the credential cache that pam_krb5 had created for the user's session would not be updated when they were renewed on the client. This update prevents pam_krb5 from creating its own cache in the scenario described, so the credential delegation mechanism is not interfered with.

BZ#700520

Prior to this update, when a client attempted to perform a password change after using a non-password-based pre-authentication mechanism (such as a Smart Card), the pam_krb5 module would unnecessarily prompt for the user's PIN (twice). This update corrects this bug.

BZ#720609, BZ#722489, BZ#733803

When a client, using SSH, logged into a remote host using the PasswordAuthentication mechanism, two credential caches would be created for the user on the remote host, but only one of them would be removed when the user logged out. This update no longer creates the second, redundant cache.

All users of pam_krb5 are advised to upgrade to this updated package, which fixes these bugs.

4.216. PAM_LDAP

4.216.1. RHBA-2011:1701 — pam_ldap bug fix update

An updated pam_ldap package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The pam_ldap package provides the pam_ldap.so module, which allows PAM-aware applications to check user passwords with the help of a directory server.

Bug Fixes

BZ#735375

All entries stored in an LDAP directory have a unique "Distinguished Name," or DN. The top level of the LDAP directory tree is the base, referred to as the "base DN". When the host option is not set the pam_ldap.so module uses DNS SRV records to determine which servers to contact to perform authentication. Prior to this update, the LDAP base "DN" option was derived from the DNS domain name, ignoring any value that had been set for "base" in the pam_ldap.conf file. As a consequence, ldap lookups failed. The "base" setting in the configuration file, pam_ldap.conf, is now correctly parsed before the configuration is read from DNS. As a result, "base" is now set to the value given in the pam_ldap.conf file and is used as the base (starting point) to search for a user's credentials.

BZ#688747

Prior to this update, pam_ldap (when called by a process which was running as root) did not re-authenticate the user during a password change operation. As a consequence, reuse of the old password was not prevented. This update backports a fix to ensure that when a privileged application initiates a password change operation, for a user whose password has expired, that the current password is again verified, allowing client-side password-quality checking to be performed when using LDAP accounts.

All users of pam_ldap are advised to upgrade to this updated package, which fixes these bugs.

4.217. PAPI

4.217.1. RHBA-2011:1755 — papi bug fix and enhancement update

An updated papi package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

PAPI (Performance Application Programming Interface) is a software library that provides access to the processor's performance-monitoring hardware.

The papi package has been upgraded to upstream version 4.1.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#705893)

All PAPI users are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.218. PARTED

4.218.1. RHBA-2011:1626 — parted bug fix and enhancement update

Updated parted packages that fix three bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The parted packages allow you to create, destroy, resize, move, and copy hard disk partitions. The parted program can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.

Bug Fixes

BZ#665496

Prior to this update, parted incorrectly calculated the position of the new partition when partitions of 1 or smaller units (eg. 1GB, 0.5GB) were created. As a result, only an extremely small partition was created. This update fixes the snap problem for 1 unit and no longer allows defining units less than 1. The value 0 is still allowed when specifying the start of the device. The next smaller units should be used instead of a value smaller than 1. eg. Use 500MB instead of 0.5GB.

BZ#692562

Prior to this update, a cylinder-head-sector (CHS) value was, under certain circumstances, especially with factory partitioned USB drives, not found. As a result, parted threw an assertion when attempting to guess the CHS used to create a partition table, even though it was safe to continue without the CHS information. This update no longer throws an assertion when it cannot guess the CHS values used to create a partition table.

BZ#746098

Prior to this update, several tests of the parted test suite failed when running as root on IBM System z and 64-bit PowerPCs. With this update, the tests run as expected.

Enhancement

BZ#711148

GPT disklabels now support the legacy_boot flag to allow bootloaders such as syslinux's hybrid gptmbr to be used on BIOS and EFI systems. It is set with the set command in parted.

All parted users are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.219. PASSWD

4.219.1. RHEA-2012:0328 — passwd enhancement update

An updated passwd package that adds two enhancements is now available for Red Hat Enterprise Linux 6.

The passwd packages contain a system utility, "passwd", which changes passwords and displays password status information using the Pluggable Authentication Modules (PAM) and Libuser libraries.

Enhancements

BZ#791139

The passwd command now supports a new option, "-e", that allows the system administrator to expire the password of the specified user so that the user is forced to change the password on the next login attempt.

BZ#791143

The passwd executable file is a setuid program so it needs to be well protected against various types of attacks. With this update, passwd has been built with the Position Independent Executables (PIE) flag, "-fPIE -pie", and the full read-only relocations (RELRO) flags, "-Wl,-z,relro,-z,now". The passwd binary is now well protected against "return-to-text" and memory corruption attacks and also against attacks based on the program's ELF section overwriting.

All users of passwd are advised to upgrade to this updated package, which adds these enhancements.

4.220. PCIUTILS

4.220.1. RHBA-2011:1760 — pciutils bug fix and enhancement update

Updated pciutils packages that fix a bug and add an enhancement are now available for Red Hat Enterprise Linux 6.

The pciutils package contains various utilities for inspecting and manipulating devices connected to the PCI bus.

Bug Fix

BZ#740630

Previously, in an attempt to free data structures from memory via the pci_free_cap() function, the "glibc detected *** double free or corruption (!prev):" error message was returned and the operation failed. A patch has been provided to address this issue and freeing system resources now works properly.

Enhancement

BZ#742223

With this update, TPH (Transaction Processing Hints) and LTR (Latency Tolerance Reporting) reporting capabilities have been added to the pciutils package to support the PCI Express 3.0 standard.

All pciutils users should upgrade to these updated packages, which fix this bug and add this enhancement.

4.221. PERL-DATE-MANIP

4.221.1. RHEA-2011:1560 — perl-Date-Manip enhancement update

An updated perl-Date-Manip package that upgrades the Date::Manip module to upstream version 6.24 is now available for Red Hat Enterprise Linux 6.

The Date::Manip module provides a mechanism for Perl scripts to perform common date or time operations, such as comparing two timestamps or parsing international times.

Enhancement

BZ#672934

Among other flaws, the previous version of the perl-Date-Manip package included outdated time zone definitions and an old API that is now considered deprecated. This update upgrades the perl-Date-Manip package to upstream version 6.24, which provides up-to-date time zone definitions and version 6 of the API. Users are still able to use the old API version 5 by explicitly using the Date::Manip::DM5 module.

All users of perl-Date-Manip are advised to upgrade to this updated package, which adds this enhancement.

4.222. PERL-NET-DNS

4.222.1. RHBA-2011:1271 — perl-Net-DNS bug fix update

An updated perl-Net-DNS package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The perl-Net-DNS package contains a collection of Perl modules that act as a Domain Name System (DNS) resolver. It allows the programmer to perform DNS queries that are beyond the capabilities of the gethostbyname and gethostbyaddr routines.

Bug Fix

BZ#688211

Prior to this update, perl-Net-DNS lacked a complete IPv6 functionality. This update adds the dependencies related to IPv6 and, in addition, prevents the possibility of interactive (re)build.

All users of perl-Net-DNS should upgrade to this updated package, which fixes this bug.

4.223. PERL-NETADDR-IP

4.223.1. RHEA-2011:0873 — perl-NetAddr-IP bug fix update

An updated perl-NetAddr-IP package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The perl-NetAddr-IP module provides an object-oriented abstraction on top of IP addresses or IP subnets, that allows for easy manipulations.

Bug Fix

BZ#692857

Prior to this update, the documentation included in the perl-NetAddr-IP module did not contain a correct description with regard to the addition of a constant to an IP address. The problem has been resolved in this update by correcting the respective part of the documentation.

All users of perl-NetAddr-IP are advised to upgrade to this updated package, which fixes this bug.

4.224. PERL-SYS-VIRT

4.224.1. RHBA-2011:1573 — perl-Sys-Virt bug fix and enhancement update

An updated perl-Sys-Virt package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The perl-Sys-Virt package provides application programming interfaces (APIs) for managing virtual machines from Perl, using the libvirt library.

Bug Fix

BZ#705792

Prior to this update, the flags argument was hardcoded to value 0 in virDomainGetXMLDesc. As a result, security sensitive domain information was not accessible using the libvirt perl bindings. This update adds the flags parameter to all get_xml_description methods. Now, the security sensitive domain information can be obtained as expected.

Enhancement

BZ#717887

The Sys::Virt module has been updated to provide support for the new APIs introduced between version 0.8.7 and 0.9.3 of the libvirt library.

All users of perl-Sys-Virt are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.225. PERL-TEST-SPELLING

4.225.1. RHBA-2011:1093 — perl-Test-Spelling bug fix update

An updated perl-Test-Spelling package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The perl-Test-Spelling package allows users to check spelling of a POD file.

Bug Fix

BZ#636835

Prior to this update, the perl-Test-Spelling package erroneously required the aspell package instead of the hunspell package at runtime. This update fixes the problem by correcting perl-Test-Spelling's runtime dependencies so that the hunspell package is now required, as expected.

All users of perl-Test-Spelling should upgrade to this updated package, which fixes this bug.

4.226. PHP

4.226.1. RHSA-2012:0019 — Moderate: php53 and php security update

Updated php53 and php packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6 respectively.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fixes

CVE-2011-4885

It was found that the hashing routine used by PHP arrays was susceptible to predictable hash collisions. If an HTTP POST request to a PHP application contained many parameters whose names map to the same hash value, a large amount of CPU time would be consumed. This flaw has been mitigated by adding a new configuration directive, max_input_vars, that limits the maximum number of parameters processed per request. By default, max_input_vars is set to 1000.

CVE-2011-4566

An integer overflow flaw was found in the PHP exif extension. On 32-bit systems, a specially-crafted image file could cause the PHP interpreter to crash or disclose portions of its memory when a PHP script tries to extract Exchangeable image file format (Exif) metadata from the image file.

Red Hat would like to thank oCERT for reporting CVE-2011-4885. oCERT acknowledges Julian Wälde and Alexander Klink as the original reporters of CVE-2011-4885.

All php53 and php users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.226.2. RHSA-2012:0093 — Critical: php security update

Updated php packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2012-0830

It was discovered that the fix for CVE-2011-4885 (released via RHSA-2012:0071, RHSA-2012:0033, and RHSA-2012:0019 for php packages in Red Hat Enterprise Linux 4, 5, and 6 respectively) introduced an uninitialized memory use flaw. A remote attacker could send a specially-crafted HTTP request to cause the PHP interpreter to crash or, possibly, execute arbitrary code.

All php users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.226.3. RHSA-2012:0546 — Critical: php security update

Updated php packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2012-1823

A flaw was found in the way the php-cgi executable processed command line arguments when running in CGI mode. A remote attacker could send a specially-crafted request to a PHP script that would result in the query string being parsed by php-cgi as command line options and arguments. This could lead to the disclosure of the script's source code or arbitrary code execution with the privileges of the PHP interpreter.

Red Hat is aware that a public exploit for this issue is available that allows remote code execution in affected PHP CGI configurations. This flaw does not affect the default configuration in Red Hat Enterprise Linux 5 and 6 using the PHP module for Apache httpd to handle PHP scripts.

All php users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.226.4. RHSA-2013:1061 — Critical: php security update

Updated php packages that fix one security issue are now available for Red Hat Enterprise Linux 5.3 Long Life, and Red Hat Enterprise Linux 5.6, 6.2 and 6.3 Extended Update Support.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2013-4113

A buffer overflow flaw was found in the way PHP parsed deeply nested XML documents. If a PHP application used the xml_parse_into_struct() function to parse untrusted XML content, an attacker able to supply specially-crafted XML could use this flaw to crash the application or, possibly, execute arbitrary code with the privileges of the user running the PHP interpreter.

All php users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.227. PHP-PEAR

4.227.1. RHSA-2011:1741 — Low: php-pear security and bug fix update

An updated php-pear package that fixes one security issue and multiple bugs is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The php-pear package contains the PHP Extension and Application Repository (PEAR), a framework and distribution system for reusable PHP components.

Security Fix

CVE-2011-1072

It was found that the "pear" command created temporary files in an insecure way when installing packages. A malicious, local user could use this flaw to conduct a symbolic link attack, allowing them to overwrite the contents of arbitrary files accessible to the victim running the "pear install" command.

Bug Fixes

BZ#651897

The php-pear package has been upgraded to version 1.9.4, which provides a number of bug fixes over the previous version.

BZ#747361

Prior to this update, php-pear created a cache in the "/var/cache/php-pear/" directory when attempting to list all packages. As a consequence, php-pear failed to create or update the cache file as a regular user without sufficient file permissions and could not list all packages. With this update, php-pear no longer fails if writing to the cache directory is not permitted. Now, all packages are listed as expected.

All users of php-pear are advised to upgrade to this updated package, which corrects these issues.

4.228. PIDGIN

4.228.1. RHSA-2011:1821 — Moderate: pidgin security update

Updated pidgin packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Pidgin is an instant messaging program which can log in to multiple accounts on multiple instant messaging networks simultaneously.

Security Fixes

CVE-2011-4601

An input sanitization flaw was found in the way the AOL Open System for Communication in Realtime (OSCAR) protocol plug-in in Pidgin, used by the AOL ICQ and AIM instant messaging systems, escaped certain UTF-8 characters. A remote attacker could use this flaw to crash Pidgin via a specially-crafted OSCAR message.

CVE-2011-4602

Multiple NULL pointer dereference flaws were found in the Jingle extension of the Extensible Messaging and Presence Protocol (XMPP) protocol plug-in in Pidgin. A remote attacker could use these flaws to crash Pidgin via a specially-crafted Jingle multimedia message.

Red Hat would like to thank the Pidgin project for reporting these issues. Upstream acknowledges Evgeny Boger as the original reporter of CVE-2011-4601, and Thijs Alkemade as the original reporter of CVE-2011-4602.

All Pidgin users should upgrade to these updated packages, which contain backported patches to resolve these issues. Pidgin must be restarted for this update to take effect.

4.229. PINENTRY

4.229.1. RHBA-2011:1096 — pinentry bug fix update

Updated pinentry packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The pinentry package contains a collection of simple PIN or password entry dialogs, which utilize the Assuan protocol as described by the Project Aegypten. The pinentry package also contains the command line version of the PIN entry dialog.

Bug Fix

BZ#677665

Prior to this update, there was a problem when entering a password using the pinentry-curses utility; an error message was displayed instead of the password entry dialog if pinentry-curses was run under a user different from the user who owned the current tty. This bug has been fixed in this update so that no error message is now displayed and pinentry-curses asks for a password as expected.

All users of pinentry are advised to upgrade to these updated packages, which fix this bug.

4.230. PIRANHA

4.230.1. RHBA-2011:1716 — piranha bug fix update

An updated piranha package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

Piranha provides high-availability and load balancing services for Red Hat Enterprise Linux. The piranha package contains various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism that provides load balancing, primarily for Web and FTP servers.

Bug Fixes

BZ#593728

Previously, failure to start a single nanny daemon could terminate all the other nanny daemons. As a result, piranha could stop routing requests to real servers if one service monitor failed. This update adds a new option in the lvs.cf file, "hard_shutdown". The old behavior is retained with the default setting of 1. If a 0 value is set, a single nanny does not kill all nannies but the system needs manual intervention.

BZ#628872

Previously, the piranha-gui init script searched for programs in the current working directory. As a consequence, SELinux Access Vector Cache (AVC) denials could be generated when starting the piranha-gui service in unusual locations without the "service" utility. The init script has been modified to avoid this problem. Now, SELinux denials are no longer logged.

BZ#703146

Adding or removing Virtual Service descriptions in the LVS configuration requires restarting the pulse daemon (service pulse reload). Prior to this update all services (running or not) were started. When reloading the pulse daemon, if a service did not have any servers defined, the pulse daemon terminated unexpectedly with a segmentation fault. With this update, only running services are restarted. Now, the pulse daemon reloads as expected.

BZ#706881

Prior to this update, terminating a nanny or an lvs daemon did not trigger a failover to the backup server. As a consequence, the load balancer stopped working. With this update, the pulse daemon shuts down if either the nanny daemon or the lvs daemon terminates. Now, the load balancer works as expected.

BZ#708036

Previously, the piranha-gui utility reported an HTTP 414 error (Request-URI Too Long) if too many virtual servers were defined. As a consequence, when trying to edit a virtual server, the error message "Too many arguments in the URL" appeared. With this update, the number of defined virtual servers does not affect the length of the URI. Now, error messages are no longer reported.

BZ#729828

This update adds the 255.255.254.0 network mask to the piranha-gui drop-down menus.

All users of piranha are advised to upgrade to this updated package, which fixes these bugs.

4.231. PKI-CORE

4.231.1. RHBA-2011:1655 — pki-core bug fix and enhancement update

Updated pki-core packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Certificate System is an enterprise software system designed to manage enterprise public key infrastructure (PKI) deployments. PKI Core contains fundamental packages required by Red Hat Certificate System, which contain the Certificate Authority (CA) subsystem.

Note: The Certificate Authority component provided by this update is not intended to be used as a standalone server. It is installed and operates as a part of the Red Hat Enterprise Identity (IPA).

Bug Fix

BZ#698796

Configuration of a certificate server failed with the following error: "Unable to retrieve CA chain: request failed with HTTP status 500". This occurred due to a race condition between the process reading the /etc/pki-ca/registry.cfg file and the restart process as registry.cfg was timestamped on startup. registry.cfg is now left unmodified on startup.

BZ#728651

On Red Hat Certificate System 8, the 64-bit pkicreate script was attempting to use libCryptoki2.so for SafeNet Luna SA and failed to load it as the library did not exist. The code has been changed and pkicreate on 64-bit platforms now uses libCryptoki2_64.so.

BZ#691076

The pkiremove command removed all instances of the CA (Certification Authority) type instead of removing only a specific instance. This occurred because pkiremove removed the registry directory /etc/sysconfig/pki/[subsystem_type] instead of removing only the registry entry for the specific instance in the /etc/sysconfig/pki/[type]/ directory. The command now removes only the respective type instance.

BZ#708075

In a NAT (Network Address Translation) environment, authentication of an IPA machine clone could fail with a NullPointerException on machine setup. This happened when the clone tried to authenticate itself with a NAT translated IP address that was different from the IP address previously used for the authentication. Therefore, the master IPA machine rejected the authentication. As the machines use a shared key throughout the connection, the IP check was redundant and has been removed.

BZ#693835

PKI provided Apache Tomcat configuration files which set "user:group" to "pkiuser:pkiuser". Therefore, the /var/log/tomcat6/catalina.out file was also owned by pkiuser. As the file needs to be owned by Tomcat 6, the TOMCAT_LOG variable has been added to the configuration files and Tomcat now uses "tomcat:tomcat" as its "user:group".

BZ#726785

The Dogtag subsystem did not detect a replication failure if the replication failed during clone setup. Therefore, Dogtag kept looking for the root directory on the directory server and got into an infinite loop as the replication failed and the root directory was never created. Dogtag now waits for the replication to finish and the problem no longer occurs.

BZ#700522

Due to changes in startup scripts, the PKI SElinux policy was not applied and tomcat6 instances ran unconfined. The startup scripts now applies the SElinux policy if enabled and tomcat6 instances now run with the restrictions defined in the policy.

Enhancements

BZ#729126

The default validity period of the default and constraint server certificates has been changed to 2 years.

BZ#689891

The number of restarts needed during installation of Dogtag Certicate Server was decreased.

BZ#689909

Several checks have been added to speed up installation of Dogtag Certificate Server.

BZ#722634

The client usage flag has been added to the caIPAserviceCert server certificate. This allows an IPA server to use the server certificate as a client certificate and authenticate itself.

BZ#737179

The pki-setup-proxy script that adds a configuration file to Apache Tomcat, updates the server.xml and CS.cfg files has been added. The script upgrades the proxy configuration of an existing IPA installation to the AJP (Apache JServ Protocol) proxy code introduced in upstream version 2.1.1.

Users should upgrade to these updated pki-core packages, which fix the bugs and add the enhancements.

4.231.2. RHBA-2012:0357 — pki-core bug fix and enhancement update

Updated pki-core packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Certificate System is an enterprise software system designed to manage enterprise public key infrastructure (PKI) deployments. pki-core contains fundamental packages required by Red Hat Certificate System, which contain the Certificate Authority (CA) subsystem.

Note: The Certificate Authority component provided by this update is not intended to be used as a standalone server. It is installed and operates as a part of Identity Management (IPA) in Red Hat Enterprise Linux.

Bug Fix

BZ#772222

When installing IPA, the installer uses 'sslget' to communicate with the CA. The server sends out a full response to the sslget client, but the client receives only 5 bytes of the encrypted stream.

Users should upgrade to these updated pki-core packages, which fix the listed bug.

4.232. PLYMOUTH

4.232.1. RHBA-2011:1766 — plymouth bug fix update

Updated plymouth packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Plymouth provides a graphical boot animation in place of the text messages that are normally displayed. Text messages are instead redirected to a log file for viewing after boot.

Bug Fixes

BZ#719569

Previously, plymouth incorrectly parsed "console" parameters that were set to "tty0" on the kernel command line. When the user had connected the serial port from another machine and rebooted the system, the boot log was not redirected to the serial console and the user could not view it as a consequence. A patch has been applied to address the issue so that users can now view the output of the boot log.

BZ#741515

Previously, plymouth did not perform proper tty clean up on some consoles if more than one line contained the "console=" parameter. The terminal was locked as a consequence and the user was not able to log in from the serial console. With this update, plymouth is modified to correctly handle multiple lines containing "console=" and users are now able to log in as expected.

All users of plymouth are advised to upgrade to these updated packages, which fix these bugs.

4.233. POLICYCOREUTILS

4.233.1. RHBA-2011:1637 — policycoreutils bug fix update

Updated policycoreutils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The policycoreutils packages contain the core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system and its policies.

Bug Fixes

BZ#662064

Due to the wrong run_init pseudo terminal (pty) handling, it was not possible to start the sshd daemon properly with the run_init utility. With this update, the bug has been fixed so that run_init now works, as expected.

BZ#666861

If the "-D" option was used with the "semanage module" command, it resulted in a traceback. With this update, the functionality that allowed removal of every single policy module from a system has been removed from the semanage utility so that the bug is now fixed.

BZ#677541, BZ#677542

Previously, the semanage(8) man page did not describe certain options. This update corrects the man page so that these options are now described, as expected.

BZ#689153, BZ#695288, BZ#696809, BZ#735044

Previously, the SELinux graphical tools and the common SELinux tools did not work on systems with SELinux disabled. This bug has been fixed by allowing the SELinux graphical tools and the common SELinux tools to run on these systems.

BZ#690502

Previously, running the "sandbox -H /tmp/testuserhome ls ~" command resulted in a traceback. With this update, the command now works as expected.

BZ#702860

Previously, the gnome-python2-gtkhtml2 package was required by the policycoreutils-gui package. As a result, the Automatic Bug Reporting Tool (ABRT) utilities generated a traceback. With this update, the gnome-python2-gtkhtml2 package is no longer required by the policycoreutils-gui package, thus the bug is fixed.

BZ#705027

Previously, the sestatus(8) man page missed the description of the "-b" option. This update corrects the man page so that this option is now described, as expected.

BZ#715021

Previously, polyinstantiated directories had the wrong multilevel secure (MLS) range set for a user. As a result, the user was not able to create files in the /tmp/ directory, or, under certain circumstances, to log in. This update fixes the bug by correcting the namespace.init script.

BZ#734467

Previously, the rsync package was not required by any of the policycoreutils packages, although the "seunshare" command, which is provided by the policycoreutils-sandbox package, requires the rsync package to work properly. With this update, the rsync package is now required by the policycoreutils-sandbox package, thus the bug is fixed.

BZ#736153

Previously, it was possible to change the USER, ROLE, and MLS ranges on an object with the "restorecon" command even if the "-F" option was not specified. This update fixes the unintended behavior by disallowing "restorecon" to change the USER, ROLE or MLS ranges on the object unless the "-F" option is specified.

BZ#739587, BZ#740669

If the "restorecon" command was successful, the return code "1" was erroneously returned. This unintended behavior has been fixed with this update so that "restorecon" now returns the code "0", as expected.

BZ#750594

If booting with the "SELinux=disabled" option set in the /etc/selinux/config file (but without specifying the "selinux=0" option at the kernel prompt), dracut output the following error:

```
dracut: /sbin/load_policy: Can't load policy: No such file or directory
```

With this update, dracut no longer outputs this error.

All users of policycoreutils are advised to upgrade to these updated packages, which fix these bugs.

4.233.2. RHBA-2012:0134 — policycoreutils bug fix update

Updated policycoreutils packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The policycoreutils packages contain the core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system and its policies.

Bug Fixes

BZ#785678

The semanage utility did not produce correct audit messages in the Common Criteria certified environment. This update modifies semanage so that it now sends correct audit events when the user is assigned to or removed from a new role.

This update also modifies behavior of semanage concerning the user's SELinux Multi-Level Security (MLS) and Multi-Category Security (MCS) range. The utility now works with the user's default range of the MLS/MCS security level instead of the lowest.

In addition, the semange(8) manual page has been corrected to reflect the current semanage functionality.

BZ#787579

The missing exit(1) function call in the underlying code of the sepolgen-ifgen utility could cause the restorecond daemon to access already freed memory when retrieving user's information. This would cause restorecond to terminate unexpectedly with a segmentation fault. With this update, restorecond has been modified to check the return value of the getpwuid() function to avoid this situation.

BZ#787605

When installing packages on the system in Federal Information Processing Standard (FIPS) mode, parsing errors could occur and installation failed. This was caused by the "/usr/lib64/python2.7/site-packages/sepolgen/yacc.py" parser, which used MD5 checksums that are not supported in FIPS mode. This update modifies the parser to use SHA-256 checksums and installation process is now successful.

All users of policycoreutils are advised to upgrade to these updated packages, which fix these bugs.

4.234. POSTGRESQL

4.234.1. RHSA-2012:0678 — Moderate: postgresql and postgresql84 security update

Updated postgresql84 and postgresql packages that fix three security issues are now available for Red Hat Enterprise Linux 5 and 6 respectively.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fixes

CVE-2012-0868

The pg_dump utility inserted object names literally into comments in the SQL script it produces. An unprivileged database user could create an object whose name includes a newline followed by an SQL command. This SQL command might then be executed by a privileged user during later restore of the backup dump, allowing privilege escalation.

CVE-2012-0867

When configured to do SSL certificate verification, PostgreSQL only checked the first 31 characters of the certificate's Common Name field. Depending on the configuration, this could allow an attacker to impersonate a server or a client using a certificate from a trusted Certificate Authority issued for a different name.

CVE-2012-0866

CREATE TRIGGER did not do a permissions check on the trigger function to be called. This could possibly allow an authenticated database user to call a privileged trigger function on data of their choosing.

These updated packages upgrade PostgreSQL to version 8.4.11, which fixes these issues as well as several data-corruption issues and lesser non-security issues. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.4/static/release.html

All PostgreSQL users are advised to upgrade to these updated packages, which correct these issues. If the postgresql service is running, it will be automatically restarted after installing this update.

4.235. POWERPC-UTILS

4.235.1. RHEA-2011:1562 — powerpc-utils bug fix and enhancement update

An updated powerpc-utils package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The powerpc-utils package provides various utilities for a PowerPC platform.

The powerpc-utils package has been upgraded to upstream version 1.2.10, which provides a number of bug fixes and enhancements over the previous version. The powerpc-utils package now provides the following new features:

BZ#694541

The page coalescing feature that provides the ability to share identical pages in physical memory among multiple logical partitions. Identical pages are consolidated into one shared read-only copy, and expanded into individual copies if an individual partition change occurs.

BZ#632705

The lparstat tool that provides the ability to display various attributes of IBM Power Logical Partitions, such as CPU and memory entitlement and other similar attributes.

Bug Fixes

BZ#698433

When removing memory from logical partition (LPAR) in Dynamic Logical Partitioning (DLPAR), the

dynamic memory manager (drmgr) did not set the memory off-line correctly. As a consequence, the kernel of the LPAR panicked. This update corrects the code so that drmgr now sets memory off-line properly, and the kernel no longer crashes when removing memory in DLPAR.

BZ#739888

The drmgr(8) manual page contained obsolete information that drmgr is a part of the ppc64-utils suite. This has been corrected, and the manual page now states that drmgr is a part of the powerpc-utils suite.

BZ#739957

The ofpathname script was not able to convert the Open Firmware device path name to the logical device name for SAN disks. With this update, ofpathname converts path names to device names correctly.

All users of powerpc-utils are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.236. POWERTOP

4.236.1. RHBA-2011:1230 — powertop bug fix update

An updated powertop package that fixes one bug is now available for Red Hat Enterprise Linux 6.

PowerTOP is a tool to detect all the software components that make a computer consume more than necessary power when idle. PowerTOP can be used to reduce power usage by running various commands on the system.

Bug Fix

BZ#698422

Previously, PowerTOP did not correctly handle the SIGWINCH signal. As a result, PowerTOP was terminated unexpectedly if the terminal window, in which PowerTOP was running, was resized. This update fixes the SIGWINCH signal handling so that PowerTOP is not unexpectedly terminated if the terminal window is resized.

All PowerTOP users are advised to upgrade to this updated package, which fixes this bug.

4.237. PRELINK

4.237.1. RHEA-2011:1768 — prelink enhancement update

An updated prelink package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The prelink utility is used to modify ELF shared libraries and executables. It reduces the number of relocations that need to be resolved at runtime, and thus enables faster start-up.

Enhancement

BZ#739460

To improve performance on AMD Family 15h processors, the prelink utility has been adapted to align 32-bit libraries on 32 KB boundaries.

All users of prelink are advised to upgrade to this updated package, which adds this enhancement.

4.238. PROCPS

4.238.1. RHBA-2011:1554 — procps bug fix update

An updated procps package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The procps package contains a set of system utilities that provide system information using the /proc file system. The procps package includes free, pgrep, pkill, pmap, ps, pwdx, skill, slabtop, snice, sysctl, tload, top, uptime, vmstat, w and watch.

Bug Fixes

BZ#692397

There was a typo in the ps(1) manual page which caused the layout of the page to break. The typo has been fixed and the ps(1) manual page is now displayed correctly.

BZ#690078

Incorrectly declared variables may have led to a memory leak or caused the pmap, ps and vmstat utilities to misbehave. The variables are now nullified and declared in the correct place, fixing the problem.

BZ#697935

Prior to this update, the sysctl utility did not accept partial keys to display all the key pairs within a certain namespace of the /proc file system. The following error message appeared when running the "sysctl net.core" command:

"Invalid argument" reading key "net.core"

With this update, the sysctl utility accepts the partial keys and all the keys with the specified prefix are now displayed.

BZ#709684

Previously, the top utility displayed incorrect values in the SWAP field due to the values of the per-process swap being incorrectly calculated as a difference between virtual and physical memory used by a task. The /proc file system provided by kernel is now the main source of the swap information.

BZ#701710

Previously, the vmstat utility displayed incorrect values of the free page count on 8TB SGI (Silicon Graphics) systems. The vmstat utility has been modified to display the correct free page count.

All users of procps are advised to upgrade to this updated package, which fixes these bugs.

4.239. PSACCT

4.239.1. RHBA-2012:1051 — psacct bug fix update

Updated psacct packages that fix two bugs are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The psacct packages contain utilities for monitoring process activities, including ac, lastcomm, accton, dump-acct, dump-utmp and sa. The "ac" command displays statistics about how long users have been logged on. The "lastcomm" command displays information about previously executed commands. The "accton" command turns process accounting on or off. The "dump-acct" command transforms the output file from the accton format to a human-readable format. The "dump-utmp" command prints utmp files in human-readable format. The "sa" command summarizes information about previously executed commands.

Bug Fixes

BZ#828726

Previously, improper data type detection could have caused an arithmetic overflow. As a consequence, the dump-acct tool reported incorrect elapsed time values. A patch has been applied so that correct values are reported with this update.

BZ#834216

Previously, improper data type conversion caused the dump-utmp tool to report invalid timestamps. Consequently, mainly on the 64-bit PowerPC architecture, dump-utmp could have terminated unexpectedly with a segmentation fault. A patch has been applied so that correct values are reported and no crashes occur with this update.

All users of psacct are advised to upgrade to these updated packages, which fix these bugs.

4.240. PULSEAUDIO

4.240.1. RHBA-2012:1066 — pulseaudio bug fix update

Updated pulseaudio packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

PulseAudio is a sound server for Linux and other Unix-like operating systems.

Bug Fix

BZ#836138

On certain sound card models by Creative Labs, the S/PDIF Optical Raw output was enabled on boot regardless of the previous settings. This caused the audio output on the analog duplex output to be disabled. With this update, the S/PDIF Optical Raw output is disabled on boot so that the analog output works as expected.

All users of pulseaudio are advised to upgrade to these updated packages, which fix this bug.

4.241. PYKICKSTART

4.241.1. RHBA-2011:1682 — pykickstart bug fix update

An updated pykickstart package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The pykickstart package contains a python library for manipulating kickstart files.

Bug Fix

BZ#656278

When validating the syntax of a kickstart file in certain locales, the ksvalidator tool terminated with a traceback if the kickstart file contained any deprecated syntax. This has been fixed: ksvalidator terminates no longer and prints a warning message that the kickstart file contains a deprecated syntax.

All users of pykickstart are advised to upgrade to this updated package, which resolves this bug.

4.242. PYPARTED

4.242.1. RHBA-2011:1641 — pyparted bug fix update

An updated pyparted package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The pyparted package contains Python bindings for the libparted library. It is primarily used by the Red Hat Enterprise Linux installation software.

Bug Fix

BZ#725558

Due to a missing flag in the GPT (Guid Partition Table) disklabel, the anaconda installer terminated with a traceback during the installation of Red Hat Enterprise Linux 6.2. With this update, support for the PARTITION_LEGACY_BOOT flag has been added to the pyparted package, thus fixing this bug.

Users of pyparted are advised to upgrade to this updated package, which fixes this bug.

4.243. PYTHON

4.243.1. RHBA-2011:1564 — python bug fix and enhancement update

Updated python packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

Python is an interpreted, interactive, object-oriented programming language.

Bug Fixes

BZ#697470

The Python standard library contains numerous APIs that handle the uid_t and gid_t attributes, which contain unsigned 32-bit values. Previously, the existing code often passed the values as C language long values, which are signed 32-bit values on 32-bit architectures. Consequently, negative integer objects occurred when a uid_t/gid_t value was equal or larger than 2^31 on 32-bit architectures. With this update, the standard library has been updated throughout to accept the full range of uid_t/gid_t values (0 through 2^32-1), using "int" objects for small values, but using "long" objects where needed to avoid integer overflow. As a special case, "-1" is also supported, as this value has special meaning for the os.chown() function and other related functions.

BZ#713082

Previously, the multiprocessing module used the "select" system call to communicate with subprocesses, limiting the number of file descriptors to the value of the FD_SETSIZE variable (1024). With this update, the multiprocessing module has been ported to use the "poll" system call, instead of

"select", thus fixing this bug.

BZ#685234

Previously, a race condition sometimes caused the forking.Popen.poll() method of the multiprocessing module to terminate with the "OSError: [Errno 10] No child processes" error message when starting subprocesses. This bug has been fixed and the crashes no longer occur in the described scenario.

BZ#689794

Previously, the getpass.getpass() method discarded Ctrl-C and Ctrl-Z input, requiring the user to press Ctrl-D to exit the password entry prompt and then returning traceback error messages. With this update, the described user input is processed properly by the getpass.getpass() method.

BZ#699740

Due to a bug, the readline.get_history_length() and readline.get_history_item() methods leaked memory when executed. This bug has been fixed and no longer occurs.

BZ#727364

When building the C extension modules, if a value for the CFLAGS variable is defined in the environment, it is appended to the compilation flags from Python's Makefile. Due to a bug, only flags stored in the OPT variable were supplied from the Makefile. Consequently, the "-fno-strict-aliasing" flag was missing and build errors occurred. This bug has been fixed, CFLAGS are properly appended to the original Python build string, and no build errors are now returned in the described scenario.

BZ#667431

When feeding data to the standard input of short-lived processes, the subprocess.Popen.communicate() method sometimes terminated with the "OSError: [Errno 32] Broken pipe" error message. This bug has been fixed and the crashes no longer occur in the described scenario.

Enhancement

BZ#711818

The gdb (GNU Debugger) Python hooks for debugging Python itself (via the python-debuginfo package) have been enhanced. The hooks now report if a thread is waiting on a lock, such as the GIL (Global Interpreter Lock), and call to appropriate C functions, methods, and garbage collections. In addition, the hooks have been optimized to provide at least file and function names, when line numbers and locals are not available.

All users of python are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.243.2. RHSA-2012:0744 — Moderate: python security update

Updated python packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

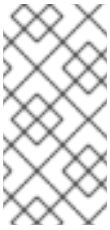
The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Python is an interpreted, interactive, object-oriented programming language.

Security Fixes

CVE-2012-1150

A denial of service flaw was found in the implementation of associative arrays (dictionaries) in Python. An attacker able to supply a large number of inputs to a Python application (such as HTTP POST request parameters sent to a web application) that are used as keys when inserting data into an array could trigger multiple hash function collisions, making array operations take an excessive amount of CPU time. To mitigate this issue, randomization has been added to the hash function to reduce the chance of an attacker successfully causing intentional collisions. ()



NOTE

The hash randomization is not enabled by default as it may break applications that incorrectly depend on dictionary ordering. To enable the protection, the new "PYTHONHASHSEED" environment variable or the Python interpreter's "-R" command line option can be used. Refer to the python(1) manual page for details.

The RHSA-2012:0731 expat erratum must be installed with this update, which adds hash randomization to the Expat library used by the Python pyexpat module.

CVE-2012-0845

A flaw was found in the way the Python SimpleXMLRPCServer module handled clients disconnecting prematurely. A remote attacker could use this flaw to cause excessive CPU consumption on a server using SimpleXMLRPCServer.

CVE-2011-4940

A flaw was found in the way the Python SimpleHTTPServer module generated directory listings. An attacker able to upload a file with a specially-crafted name to a server could possibly perform a cross-site scripting (XSS) attack against victims visiting a listing page generated by SimpleHTTPServer, for a directory containing the crafted file (if the victims were using certain web browsers).

CVE-2011-4944

A race condition was found in the way the Python distutils module set file permissions during the creation of the .pypirc file. If a local user had access to the home directory of another user who is running distutils, they could use this flaw to gain access to that user's .pypirc file, which can contain usernames and passwords for code repositories.

Red Hat would like to thank oCERT for reporting CVE-2012-1150. oCERT acknowledges Julian Wälde and Alexander Klink as the original reporters of CVE-2012-1150.

All Python users should upgrade to these updated packages, which contain backported patches to correct these issues.

4.244. PYTHON-DMIDECODE

4.244.1. RHBA-2011:1589 — python-dmidecode bug fix update

An updated python-dmidecode package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The python-dmidecode package provides a python extension module that uses the code-base of the dmidecode utility and presents the data as python data structures or as XML data using the libxml2 library.

The python-dmidecode package has been upgraded to upstream version 3.10.13, which provides a number of bug fixes over the previous version. (BZ#621567)

Bug Fixes

BZ#627901

When trying to identify the processor type by performing a string comparison, Python terminated with a segmentation fault. This was caused by DMI tables which did not report the CPU processor information as a string and returned a NULL value instead. This update adds additional checks for NULL values before doing the string comparison.

BZ#646429

Previously, when calling the memcpy() function on the IBM System z machine which was under heavy memory load, a SIGILL signal was triggered. As a consequence, the complete Python interpreter core dumped. A signal handler was added to properly handle heavy memory loads.

BZ#667363

Prior to this update, when running the rhn_register utility, providing a valid user name and password, and clicking the Forward button, the tool terminated unexpectedly with a segmentation fault. This was caused by the dmi_processor_id() function not checking whether the version pointer was NULL. This update adds additional checks for NULL values, fixing the problem.

All users of python-dmidecode are advised to upgrade to this updated package, which resolves these bugs.

4.245. PYTHON-MEH

4.245.1. RHBA-2011:1763 — python-meh bug fix update

An updated python-meh package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The python-meh package provides a python library for handling exceptions.

Bug Fixes

BZ#728871

Prior to this update, bug reports filed with python-meh were missing information. With this update, these bug reports now include more useful information on system architecture and versions of packages related to the bug.

BZ#730924

Prior to this update, the report packages which python-meh depended on were named "report-gtk" and "report-newt". The packages have been renamed "libreport-gtk" and "libreport-newt". This update changes the python-meh spec file to require these new report packages.

All users of python-meh are advised to upgrade to this updated package, which fixes these bugs.

4.246. PYTHON-NETADDR

4.246.1. RHBA-2011:1658 — python-netaddr bug fix update

An updated python-netaddr package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The python-netaddr package provides a network address representation and manipulation library for Python. The netaddr library allows Python applications to work with IPv4 and IPv6 addresses, subnetworks, non-aligned IP address ranges and sets, MAC addresses, Organizationally Unique Identifiers (OUI), Individual Address Blocks (IAB), and IEEE EUI-64 identifiers.

Bug Fix

BZ#710373

Prior to this update, if an IPNetwork object was instantiated with bad data, the python-netaddr code tried to access an unbound local variable and the erroneous exception "UnboundLocalError" was raised. It should raise the AddrFormatError exception instead. Consequently a user of python-netaddr had to check for all exceptions instead of just "netaddr.core.AddrFormatError". With this update the code is corrected and functions as expected in the scenario described.

All users of python-netaddr are advised to upgrade to this updated package, which fixes this bug.

4.247. PYTHON-PSYCOPG2

4.247.1. RHBA-2012:0145 — python-psycopg2 bug fix and enhancement update

An updated python-psycopg2 package that fixes multiple bugs and adds multiple enhancements is now available for Red Hat Enterprise Linux 6.

The python-psycopg2 package provides a PostgreSQL database adapter for the Python programming language.

The python-psycopg2 package has been upgraded to upstream version 2.0.14, which provides a number of bug fixes and enhancements over the previous version, including the fix for a memory leak in cursor handling. This update also ensures better compatibility with the PostgreSQL object-relational database management system version 8.4. (BZ#787164)

All users of python-psycopg2 are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.248. PYTHON-QPID

4.248.1. RHBA-2011:1666 — python-qpid bug fix update

An updated python-qpid package is now available for Red Hat Enterprise Linux 6.

The python-qpid package provides a python client library for the Apache Qpid implementation of the Advanced Message Queuing Protocol (AMQP).

The python-qpid package has been upgraded to upstream version 0.12. (BZ#706993)

Users of python-qpid are advised to upgrade to this updated package.

4.249. PYTHON-RHSM

4.249.1. RHBA-2011:1696 — python-rhsm bug fix update

An updated python-rhsm package that fixes multiple bugs is now available for Red Hat Enterprise Linux 6.

The python-rhsm package contains a small library for communicating with the representational state transfer (REST) interface of a Red Hat Unified Entitlement Platform. This interface is used for the management of system entitlements, certificates, and access to content.

Bug Fixes

BZ#700601

Prior to this update, the firstboot utility was trying to set an erroneous environment variable LANG=us. As a result, firstboot was unable to start properly. With this update, the C locale is now used as the fallback locale so that the problem does not occur anymore.

BZ#719378

If a user name containing a white space was submitted during the registration process in the Subscription Manager, an incorrect error message was displayed. This problem has been fixed in this update so that the correct error message "Invalid credentials" is now displayed.

BZ#728266

If a subscription was selected in the My Subscriptions tab in the Subscription Manager, and then the Unsubscribe button was pressed, an error occurred. With this update, the problem has been fixed so that the unsubscribe function in the Subscription Manager now works, as expected.

BZ#736166

The /etc/rhsm/ca/candlepin-stage.pem, /etc/rhsm/ca/fakamai-cp1.pem, and /etc/rhsm/ca/redhat-uep.pem certificates have been moved to the updated python-rhsm package so that it is now possible for python-rhsm to register with the hosted Candlepin system.

BZ#746241

If the rhsmcertd daemon received information about an existing update, but no products were installed, an exception occurred. Also, if the virt-who agent attempted to update the guest systems of a host, but there were no guest systems available, an exception occurred.

All users of python-rhsm are advised to upgrade to this updated package, which fixes these bugs.

4.250. PYTHON-SLIP

4.250.1. RHBA-2012:0413 — python-slip bug fix update

Updated python-slip packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Simple Library for Python (SLIP) packages contain miscellaneous code for convenience, extension and workaround purposes.

The python-slip packages have been upgraded to upstream version 0.2.20, which provides a number of bug fixes over the previous version. In addition, this update fixes a bug causing previous versions of

python-slip to incorrectly determine whether SELinux was enabled or not. Therefore, convenience functions for writing files always attempted to set SELinux labels even if SELinux was disabled. This could cause for example the system-config-date tool to fail to change settings. (BZ#796323)

All users of python-slip are advised to upgrade to these updated packages, which fix this bug.

4.251. PYTHON-SQLALCHEMY

4.251.1. RHSA-2012:0369 — Moderate: python-sqlalchemy security update

An updated python-sqlalchemy package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

SQLAlchemy is an Object Relational Mapper (ORM) that provides a flexible, high-level interface to SQL databases.

Security Fix

CVE-2012-0805

It was discovered that SQLAlchemy did not sanitize values for the limit and offset keywords for SQL select statements. If an application using SQLAlchemy accepted values for these keywords, and did not filter or sanitize them before passing them to SQLAlchemy, it could allow an attacker to perform an SQL injection attack against the application.

All users of python-sqlalchemy are advised to upgrade to this updated package, which contains a patch to correct this issue. All running applications using SQLAlchemy must be restarted for this update to take effect.

4.252. PYTHON-VIRTINST

4.252.1. RHBA-2011:1643 — python-virtinst bug fix and enhancement update

An updated python-virtinst package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The python-virtinst package provides a Python module that helps build and install libvirt-based virtual machines.

The python-virtinst package has been upgraded to upstream version 0.600.0, which provides a number of bug fixes and enhancements over the previous version. In particular, this update fixes the following bugs:

BZ#684786

Prior to this update, optimal cache and asynchronous I/O defaults were applied when a virtual machine was created, but not when a new device was added to an existing guest. This negatively affected the performance of such devices. With this update, the underlying source code has been corrected to apply the optimized defaults to new disks for existing guests as well.

BZ#696969

The virtinst module for Python often called the ifconfig program unnecessarily when parsing a domain XML file. Consequent to this, if a domain contained many "direct" network interfaces, the virt-manager application responded so slowly that it could not be used properly. This update removes the redundant ifconfig calls from the code, and virt-manager now works well even with a large number of "direct" network interfaces.

BZ#697798

When using the virt-install utility, an attempt to use the "--location" (or "-l") command line option to specify an ISO image file rendered the guest unable to find this image during installation. This update corrects the underlying source code to make sure such guests can now find the ISO image as expected.

BZ#698085

When the user attempted to use the virt-install utility to specify a static SELinux label, the utility failed to create correct guest configuration and the static SELinux label did not take effect for this guest. This update ensures that virt-install now generates correct configuration so that the static labels can be set as expected.

BZ#727986

When the user attempted to run the virt-install command with a mixed-case value of the "--cpu" option, the previous version of the virt-install utility failed with an error, because it automatically converted values passed on the command line to lower case. This update corrects the utility to preserve the case of command line arguments, and the "virt-install --cpu" command can now be run with a mixed-case value as expected.

BZ#742736

Due to the virt-install utility not specifying any clock policy for Windows guests, the time on the guest could skew from the time on the host. To prevent this, this update adapts the virt-install utility to specify the tickpolicy "catchup".

Enhancements

BZ#691304

A new "--disk device=cdrom" command line option is now supported by the virt-install utility. This option allows the user to specify a CD-ROM or diskette drive without inserted media.

BZ#691331

A new "--numatune" command line option is now supported by the virt-install utility. This option allows the user to specify the Non-Uniform Memory Access (NUMA) nodes for memory pinning.

BZ#693876

The virt-install utility can now be used to create Linux container guests. This includes application containers and full OS containers. Note that no tool is provided for creating an OS directory tree and users must build this tree manually.

All users of python-virtinst are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.253. QEMU-KVM

4.253.1. RHSA-2011:1531 — Moderate: qemu-kvm security bug fix and enhancement update

Updated qemu-kvm packages that fix one security issue, multiple bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems that is built into the standard Red Hat Enterprise Linux kernel. The qemu-kvm packages form the user-space component for running virtual machines using KVM.

Security Fix

CVE-2011-2527

It was found that qemu-kvm did not properly drop supplemental group privileges when the root user started guests from the command line ("/usr/libexec/qemu-kvm") with the "-runas" option. A qemu-kvm process started this way could use this flaw to gain access to files on the host that are accessible to the supplementary groups and not accessible to the primary group.

NOTE

This issue only affected qemu-kvm when it was started directly from the command line. It did not affect the Red Hat Enterprise Virtualization platform or applications that start qemu-kvm via libvirt, such as the Virtual Machine Manager (virt-manager).

Bug Fixes

BZ#699635

When the "virsh dump" command was executed with the "--live" option, the subsequent "virsh dump" command for the same domain could misbehave. This was caused by a function trying to deallocate memory that had already been freed. To avoid this issue, the log field of the vhost device structure is now set to NULL after it has been passed to a deallocating routine. Running the "virsh dump" command repeatedly no longer leads to non-standard behavior, and the core dump of a guest is now collected.

BZ#697441

Previously, SPICE (the Simple Protocol for Independent Computing Environments) sent the QMP events from the SPICE worker thread context unlocked. As a consequence, memory corruption occurred in certain cases. Global QEMU lock is now taken before the QMP events are sent, which fixes the problem.

BZ#690427

When the user installed a previous version of Windows QXL driver without the off-screen support over a new driver, the virtual machine terminated unexpectedly when the user attempted to switch to graphics mode. With this update, the update_area_surface variable is nullified on the reset of the QXL device, and virtual machines successfully load with a previous version of the driver.

BZ#711213

Previously, the NFS (Network File System) request for the direct vectored I/O operation resulted in splitting a single I/O request into multiple requests. This had a significant impact on performance. QEMU has been modified to detect files that exist in NFS when a request for vectored I/O operation comes to the server. The QEMU_AIO_MISALIGNED flag is now used to force such requests to be handled with a linear buffer.

BZ#720972

The Broadcom Corporation NetXtreme BCM5761 Gigabit Ethernet PCIe network controller provides a PCI-Express Cap structure that is 8 bytes shorter than it should be according to the PCI-Express 2.0 specification. This resulted in memory corruption when it was allocated for device assignment. The code has been modified to accept the reduced size of the structure. BCM5761 can now be successfully re-assigned.

BZ#721114

Prior to this update, the savevm file was not flushed to disk properly. Restoring a virtual machine failed in certain cases due to the savevm file being incomplete. The fsync() call has been added to flush the data to disk, which fixes the problem.

BZ#730587

The qemu-img tool tried to keep sparseness even on very small areas, issuing small write requests. As a consequence, executing the "qemu-img convert" command took a long time for certain images. The qemu-img tool now requires larger zero areas to keep sparseness. Too small write requests are now avoided, and the "qemu-img convert" command converts images in a reasonable time.

BZ#728905

If the "none" cache option was selected, all the writes to the destination were very small. To improve the performance of qemu-img, the tool has been modified to use larger buffers so that the writes to the destination are larger.

BZ#718664

Previously, migration of floppy images failed if the user migrated an image from a newer version of qemu-kvm to an older version, because qemu-kvm met a subsection it did not recognize. In order to keep the migration compatibility, qemu-kvm now accepts the subsections it does not recognize. As a result, migration of floppy images between any versions of qemu-kvm is successful.

BZ#733010

When canceling a USB packet, the usb-storage emulation tried to cancel the corresponding SCSI (Small Computer Systems Interface) request without checking whether one existed. A NULL pointer dereference caused QEMU to terminate with a segmentation fault. Checks are now performed to determine the presence of the SCSI request. Non-existing requests are not referenced any more.

BZ#728464

If the user started QEMU with the "-no-shutdown" option, asking QEMU not to quit after the guest shutdown, the flag was overlooked after the first shutdown of the guest. QEMU has been modified to accept the option after repetitive shutdowns. QEMU no longer quits if this option is supplied.

BZ#707130

When KVM guests were launched with the "-device isa-serial" option instead of the "-serial" option, serial devices created were not visible by Windows guests. This was due to QEMU not exposing these devices in the guests' Advanced Configuration and Power Interface (ACPI) tables. With this

update, the guest's ACPI Differentiated System Description Table (DSDT) now properly determines the presence of serial devices, and Windows guests can now see them properly.

BZ#694378

Previously, invalid balloon values, for example 0, caused QEMU to terminate. With this update, input is validated, and QEMU does not terminate if invalid input occurs.

BZ#676528

Previously, the tray got locked if the user ejected a medium forcibly, by executing the "eject -f" command. As a consequence, the user was unable to insert new media afterward. QEMU has been modified to leave the tray open so that users can insert new media as expected.

BZ#624983

Previously, QEMU did not support the new set of Model Specific Registers (MSR), and guests that used only the new set were therefore not able to use kvmclock. The new MSR set is now supported, and all guests are now able to use kvmclock.

BZ#737921

Previously, a SPICE client connected to the migration target only if the migration was completed. However, the ticket on the target was set before the migration started. If the time of the migration was longer that the time for which the ticket expired, the SPICE client failed to connect to the target and terminated. The SPICE server now informs the SPICE client to connect to the target before the migration starts. The SPICE server waits until the client performs the initial connection, and then calls the completion callback of the "client_migrate_info" command. Now, the SPICE client connects to the migration target after the migration.

BZ#710349

Previously, specifying serial numbers for virtio block devices did not work as expected. Patches have been applied to address this issue; virtio block disks are now correctly identified by guests and can be found in the /dev/disk/by-id/ directory.

BZ#738565

A bug in KVM's Non-Maskable Interrupt (NMI) delivery mechanism caused kernel dumps not to be taken on SMP guests. The bug has been fixed, and kernel dumps are now successfully captured on SMP guests.

BZ#706711

Suspending a Windows virtual machine with the running QXL driver caused the machine to terminate on resume. This update implements related I/O calls, and handling specific for S3 adapters in the driver (note that the future QXL driver is required). A Windows virtual machine with the running QXL driver can now be correctly suspended and resumed.

BZ#700134

Prior to this update, the QXL driver submitted requests to the SPICE server thread and waited synchronously for the result. This, in certain cases, caused qemu-kvm to be unresponsive for a long time. With this update, completion notification is used instead of waiting. SPICE server thread processes the requests asynchronously, and qemu-kvm no longer hangs.

BZ#742484

Previously, drives with removable media were ignored when creating snapshots. As a consequence,

reverting to a certain snapshot did not revert writes to floppy disks. A patch has been applied to ensure that only read-only drives with read-only or empty media are ignored. Snapshotting now treats writable floppy disks like any other writable drive.

BZ#742480

Previously, if the guest applied the "eject" command with the "-i" parameter to lock an open tray, the guest was afterward not able to close the tray by running the "eject -t" command. A patch has been applied to address this issue so that guests can successfully close open trays, even if they are locked.

BZ#694373

When specifying a negative balloon value, the value was recognized by the code as a very high positive value. As a consequence, the RAM the guest was started with, increased to its maximum. With this update, QEMU now checks for negative values, and reports them as an error.

BZ#742476

Previously, the "eject -f" monitor command worked even for non-removable drives. If the user used the command for such drives, the drive could not be used by the guest. Users could incorrectly interpret the problem as a hardware failure. A patch has been applied to address this issue, and qemu-kvm refuses to eject non-removable drives.

BZ#742469

Previously, the CD-ROM drive prevented the guest from locking an empty tray. With this update, qemu-kvm has been modified so that guests are allowed to lock empty drives regardless of whether a medium is present in the drive or not.

BZ#681736

Previously, after a virtio-serial port was unplugged, all the communication from the guest to the host, for all other ports on the virtio-serial device, was stopped. This was because the back ends of the ports on the device were incorrectly marked as NULL. With this update, the back ends of the device are checked per-port.

BZ#678729

When performing a device assignment of a PCI(e) PF (Physical Function) or VF (Virtual Function) device with an invalid host PCI configuration address, such as 0Z:88.00, to a KVM guest, the guest terminated with a core dump. With this update, the value of the B:D.F fields of an assigned device are now checked to ensure that they are in the proper ranges. When performing a device assignment of a PCI(e) PF or VF device with an invalid host PCI configuration address, QEMU displays an error message and the device terminates correctly.

BZ#725625

Previously, it was possible to expose multiple balloon devices to the guest. As a consequence, QEMU could misbehave if various balloon devices were given different commands. With this update, only one balloon device is allowed to be exposed to the guest. Now, QEMU works correctly.

BZ#739480

Due to wrong initialization order for some data structures, migration could fail in rare cases, and the instance of QEMU on the receiving host would terminate with a segmentation fault. The initialization code is fixed with this update, and QEMU no longer crashes.

BZ#632299

Constant polling of a device (such as a USB tablet) in the USB emulation consumed an excessive amount of CPU time. The remote wake up support has been added, which allows the guest's power management to suspend the USB devices and wait for the wake up notification. USB polling can now be stopped, and the CPU utilization on the host is therefore reduced.

BZ#720535

If the character device on the host side was connected to a virtio-serial port, and was closed just before the guest sent data, QEMU terminated unexpectedly. With this update, 0 is used as the return value of the write operation, and indicates that nothing was written to the character device.

BZ#734860

Previously, the missing NULL check caused qemu-kvm to terminate unexpectedly shortly after the start if a socket character device was missing the host parameter. This update adds the missing NULL check. Now, if the device is missing the host parameter, qemu-kvm terminates with an appropriate error message.

BZ#736975

Prior to this update, qemu-kvm failed to unregister balloon devices when hot unplugging the device. As a consequence, the user was not able to hot plug a balloon device after he had hot unplugged the previous one. With this update, qemu-kvm is modified to correctly unregister the balloon device from the balloon core in QEMU. Now, balloon devices can be added and removed successfully.

BZ#655719

Previously, the "change" monitor command did not return any error information if opening a file failed. When the user attempted to execute the "change" command to change or insert a non-existent file into the CD-ROM drive of a virtual machine, an "undefined error" or no error message would be reported. With this update, the "change" command correctly returns error information so that the user is properly informed.

BZ#658467

Every time the user executed the "savevm" command, qemu-kvm queried the value of kvmclock even if the virtual machine had been stopped. As a consequence, the stability of migration results could be broken. This update introduces a new kvmclock device, and qemu-kvm queries kvmclock only if the valid flag is set. Now, kvmclock is stable for the migration unit-test.

BZ#645351

Previously, QEMU did not support the USB 2.0 EHCI (Extended Host Controller Interface) devices. It was therefore impossible to use such devices in guests. This update adds support for the USB 2.0 EHCI emulation, so that users can use USB 2.0 devices.

BZ#583922

The RTL8139 network interface controller (NIC) emulated by qemu-kvm did not support IEEE 802.1Q-tagged frames. Guests which used 802.1Q tagged virtual LAN (VLAN) were not able to communicate with each other as a consequence. This update adds support for 802.1Q. Now, guests can use the 802.1Q VLAN protocol with RTL8139.

BZ#728984

When a QXL device is initialized, it ensures that its corresponding command rings are empty. After migration, before a virtual machine is started, and when the QXL device is initialized, the command rings should not be empty. Prior to this update, the command ring was not empty and QEMU

terminated with an assertion. With this update, QEMU is modified to ensure that the rings are empty only if the virtual machine is not stopped. Now, QEMU no longer terminates in the scenario described.

BZ#729294

Previously, the state of the keyboard LED lights was not kept during migration. When migrating a guest with, for example, Caps Lock or Num Lock turned on, the lights were turned off after the guest had been migrated, even when the function was still active. This update adds the state of the keyboard LED lights to the qemu state which is kept during migrations. As a result, the state of the keyboard LED lights is kept.

BZ#729621

Pausing all virtual CPUs was previously done by means of a specially registered handler in the vkm_vm_state_change_handler list. During migration, the source virtual machine that was stopped received an I/O exit after it's state change handler had been called, but before the virtual CPUs were paused. This resulted in an assertion and a termination of the virtual machine. With this update, the virtual CPU is paused after (or resumed before) all handlers are called. Migrations now proceed and finish as expected.

BZ#725965

During migration, the SPICE server on the target virtual machine started with the guest agent disconnected, and was not notified when the agent was connected. After the migration had been completed, the mouse on the client side was no longer available and the function of copying and pasting did not work. With this update, the guest_open() callback function is called at the migration target. Now, the mouse and the function of copying and pasting work as expected in the scenario described.

BZ#733993

Previously, the SPICE server could be started even if the ssd.running property was set to false. As a consequence, the migration target terminated unexpectedly with an assertion after the migration had been completed. To fix this problem, the ssd.running property is now set to true before the SPICE server is started.

BZ#735716

Previously, the qemu utility could be terminated by another process. The virtual machine terminated and the user was alerted. However, the event was never logged, and the user was therefore not able to determine what process caused qemu to terminate. Now, such information is logged for troubleshooting purposes.

BZ#723270

Previously, management applications were not able to determine whether the tray was open or closed. It could therefore be difficult for such applications to change media for the guest at the right time. With this update, the "info block" monitor command is extended to display the status of the tray. Management applications can now poll the command to see when the tray opens and closes.

BZ#744780

In rare cases, QEMU used a SCSI request after its memory had been freed. As a consequence, QEMU terminated unexpectedly with a segmentation fault. To fix this problem, SCSI requests are used by QEMU as a part of emulation of USB mass storage devices.

BZ#740547

Previously, the QXL memory slots were not created after migration if the migration started in VGA mode, and the guest was actually a native guest temporarily in VGA mode. After the migration had been completed, qemu-kvm terminated when the user switched from VGA mode back to native mode. With this update, all active memory slots are recreated during migration in VGA mode. Switching back to native mode is now successful after migration.

BZ#714773

Due to a missing probe marker for the qemu.kvm.qemu_vmalloc probe point, it was not possible to use "probe qemu.kvm.qemu_vmalloc" on a SystemTap script. The marker has been added to the qemu_vmalloc() function, so that now it is possible to use "probe qemu.kvm.qemu_vmalloc" on a SystemTap script

BZ#710046

Previously, qemu-kvm printed an unnecessary warning about the CPU model used. This message has been removed with this update.

BZ#705070

Previously, users were not able to take screenshots of secondary QXL displays. This update introduces a new monitor command to fix the problem.

BZ#743269

Hot unplugging a snapshot block device could cause future snapshot operations to misbehave or terminate unexpectedly. A patch has been applied to address this issue, and hot unplugging block devices no longer endangers future snapshot operations.

BZ#743342

Previously, the state of the CD-ROM tray was not migrated and got lost. The tray was instead closed and locked during the migration. This problem has been fixed and the state of the tray is migrated correctly.

BZ#701442

Previously, the vm_running variable was not explicitly initialized, and its values were only set by the state change notifier. This could confuse the virtio devices which were being hot plugged, such as virtio-net with the vhost back end. These could assume that the virtual machine was not running. As a consequence, vhost-net was not started after the virtio-net devices were hot plugged. The vm_running variable is now initialized explicitly during the virtio_common_init() call. The vhost-net devices are started, if required, after the virtio-net devices have been hot plugged.

BZ#738487

Previously, when shutting down qemu-kvm due to the SIGTERM request, qemu-kvm did not terminate if "-no-shutdown" option was used. The SIGTERM request could not be properly used to terminate qemu-kvm, and libvirt was therefore forced to send the SIGKILL signal, which could in certain cases cause disk corruption. The source code has been modified, so that the SIGTERM signal can now be used to terminate qemu-kvm even if "-no-shutdown" is used. This prevents disks from being corrupted due to the SIGKILL signal being sent.

BZ#669581

Prior to this update, functions in the migration code did not handle and report errors correctly. As a consequence, migration never ended if connection to the destination migration port was rejected (for example by a firewall). This update includes multiple fixes of error detection, reporting, and handling

of errors in the migration code. Now, handling of errors during migration is more reliable; for example if the connection to the destination migration port is rejected, this is properly detected and migration is aborted.

BZ#715017

Previously, QEMU did not provide any mechanism to report read and write latency of a block device. The management system was therefore not able to report what the average latency for block devices of virtual machines was. This update implements a mechanism so that qemu-kvm reports disk latency statistics by executing the "info blockstats" command.

BZ#710943

With this update, the event index feature is now supported by the Red Hat Enterprise Linux 6.2 guests. This reduces CPU utilization per megabyte for most workloads. The feature is turned on by default, and can be disabled in libvirt's XML configuration.

BZ#700859

Prior to this update, the memory API was used incorrectly. As a consequence, a hot plugged virtio-net device with vhost enabled became unresponsive after the guest had been paused. This problem has been fixed, and if the guest is paused, the hot plugged device works as expected.

BZ#738555

Nested virtualization is not supported by qemu-kvm. This update therefore removes the "-enable-nested" option.

BZ#723864

With this update, emulation of the following USB devices is disabled: usb-wacom-tablet (usb-tablet can be used instead), usb-braille, usb-serial, usb-net, and usb-bt-dongle.

Enhancements

BZ#716906

A new QEMU machine type, Red Hat Enterprise Linux 6.2, has been added with this update. This type is now used by default. If live migration compatibility with previous Red Hat Enterprise Linux hosts is required, users can choose the Red Hat Enterprise Linux 6.1 or Red Hat Enterprise Linux 6.0 machine types instead.

BZ#684949

Prior to this update, qemu-kvm was not able to display BIOS messages on boot of the virtual machine. With this update, sgabios support has been added to qemu-kvm, and a requirement to the new sgabios RPM package has been added as well. Now, qemu-kvm is able to use sgabios to print BIOS messages to a virtual serial device, if configured to do so.

BZ#713743

The qemu-img tool was writing disk images using writeback and filling up the cache buffers which were then flushed by the kernel. This prevented other processes from accessing the storage. In cluster environment, accessing the storage within certain timeouts could be critical. This update adds an option to choose a cache method when writing disk images. Users that require other cache methods can now choose the cache method on the command line when using qemu-img.

BZ#725054

The warning message about the ability to run qemu-kvm directly has been modified to be more clear.

BZ#621482

Previously, the qemu-img tool did not provide information about the completion percentage. This update introduces the new "-p" option for qemu-img which displays progress information while running.

BZ#696102

When resetting error physical memory pages (marked as HWPoison) of a guest, the guest tried to reuse the memory pages after reboot. As a consequence, in certain cases, the guest terminated unexpectedly, and could terminate repeatedly after multiple reboots. With this update, memory marked as HWPoison is unmapped so that is cannot be reused. After reboot, the guest can access new memory pages which are not marked as HWPoison.

BZ#693645

Newer versions of the SPICE client and agent allow users to copy and paste from the client to the guest. However, this is not desirable in all environments. This update introduces a new option, "disable-copy-paste" which allows users to turn off the copy and paste support for the virtual machine which is being started.

Users of qemu-kvm are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements. After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

4.253.2. RHSA-2011:1777 — Important: qemu-kvm security update

Updated qemu-kvm packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. qemu-kvm is the user-space component for running virtual machines using KVM.

Security Fix

CVE-2011-4111

A flaw was found in the way qemu-kvm handled VSC_ATR messages when a guest was configured for a CCID (Chip/Smart Card Interface Devices) USB smart card reader in passthrough mode. An attacker able to connect to the port on the host being used for such a device could use this flaw to crash the qemu-kvm process on the host or, possibly, escalate their privileges on the host.

All users of qemu-kvm should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

4.253.3. RHSA-2012:0050 — Important: qemu-kvm security, bug fix, and enhancement update

Updated qemu-kvm packages that fix one security issue, one bug, and add one enhancement are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. qemu-kvm is the user-space component for running virtual machines using KVM.

Security Fix

CVE-2012-0029

A heap overflow flaw was found in the way QEMU-KVM emulated the e1000 network interface card. A privileged guest user in a virtual machine whose network interface is configured to use the e1000 emulated driver could use this flaw to crash the host or, possibly, escalate their privileges on the host.

Red Hat would like to thank Nicolae Mogoreanu for reporting this issue.

Bug Fix

BZ#767721

qemu-kvm has a "scsi" option, to be used, for example, with the "-device" option: "-device virtio-blk-pci,drive=[drive name],scsi=off". Previously, however, it only masked the feature bit, and did not reject SCSI commands if a malicious guest ignored the feature bit and issued a request. This update corrects this issue. The "scsi=off" option can be used to mitigate the virtualization aspect of CVE-2011-4127 before the RHSA-2011:1849 kernel update is installed on the host.

This mitigation is only required if you do not have the RHSA-2011:1849 kernel update installed on the host and you are using raw format virtio disks backed by a partition or LVM volume.

If you run guests by invoking /usr/libexec/qemu-kvm directly, use the "-global virtio-blk-pci.scsi=off" option to apply the mitigation. If you are using libvirt, as recommended by Red Hat, and have the RHBA-2012:0013 libvirt update installed, no manual action is required: guests will automatically use "scsi=off".

NOTE

After installing the RHSA-2011:1849 kernel update, SCSI requests issued by guests via the SG_IO IOCTL will not be passed to the underlying block device when using raw format virtio disks backed by a partition or LVM volume, even if "scsi=on" is used.

Enhancement

BZ#767906

Prior to this update, qemu-kvm was not built with RELRO or PIE support. qemu-kvm is now built with full RELRO and PIE support as a security enhancement.

All users of qemu-kvm should upgrade to these updated packages, which correct these issues and add this enhancement. After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

4.253.4. RHBA-2012:0572 — qemu-kvm bug fix update

Updated qemu-kvm packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. The qemu-kvm packages form the user-space component for running virtual machines using KVM.

Bug Fixes

BZ#799002

Previously, QEMU did not support 2000x2000 screen resolution. This resolution is now supported.

BZ#805550

Previously, the free() function was missing in management of the "xsave" processor state. This led to memory leaks in qemu-kvm when a guest used the xsave functionality, causing excessive memory consumption on the host. Buffers used to manage xsave support are now freed after use so that qemu-kvm no longer leaks memory.

All users of qemu-kvm are advised to upgrade to these updated packages, which fix these bugs. After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

4.254. QL2400-FIRMWARE

4.254.1. RHBA-2011:1661 — ql2400-firmware bug fix and enhancement update

An updated ql2400-firmware package that provides several bug fixes and enhancements is now available for Red Hat Enterprise Linux 6.

The ql2400-firmware provides the firmware required to run the QLogic 2400 Series of mass storage adapters.

This update upgrades the ql2400 firmware to upstream version 5.06.02, which provides a number of bug fixes and enhancements over the previous version. (BZ#730814)

All users of QLogic 2400 Series Fibre Channel adapters are advised to upgrade to this updated package.

4.255. QL2500-FIRMWARE

4.255.1. RHBA-2011:1660 — ql2500-firmware bug fix update

An updated ql2500-firmware package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The ql2500-firmware package provides the firmware required to run the QLogic 2500 Series of mass storage adapters.

This update upgrades the ql2500 firmware to upstream version 5.06.02, which provides a number of bug fixes and enhancements over the previous version. (BZ#730818)

All users of QLogic 2500 Series Fibre Channel adapters are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.256. QPID

4.256.1. RHEA-2012:0530 — Qpid bug fix and enhancement update

Updated Qpid packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Apache Qpid is a reliable, cross-platform, asynchronous messaging system that supports the Advanced Message Queuing Protocol (AMQP) in several common programming languages. The qpid-cpp packages provide a message broker daemon that receives, stores and routes messages using the open AMQP messaging protocol along with run-time libraries for AMQP client applications developed using Qpid C++. Clients exchange messages with an AMQP message broker using the AMQP protocol. The qpid-qmf packages provide an extensible management framework layered on Qpid messaging. The qpid-tools package provides management and diagnostic tools for Apache Qpid brokers and clients. The qpid-tests package contains conformance tests for Apache Qpid. The python-qpid package provides a python client library for the Apache Qpid implementation of the AMQP protocol.

The qpid-cpp, qpid-qmf, qpid-tools, qpid-tests and python-qpid packages have been upgraded to upstream version 0.14, which provide a number of bug fixes and enhancements over the previous version. (BZ#807935, BZ#807936, BZ#807943, BZ#807946, BZ#807948)

All users of Qpid are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.257. QPID-CPP

4.257.1. RHBA-2011:1670 — qpid-cpp bug fix and enhancement update

Updated qpid-cpp packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The qpid-cpp packages provide a message broker daemon that receives, stores, and routes messages using the open AMQP (Advanced Message Queuing Protocol) messaging protocol along with runtime libraries for AMQP client applications developed using Qpid C++. Clients exchange messages with an AMQP message broker using the AMQP protocol.

The qpid-cpp package has been upgraded to upstream version 0.12, which provides numerous bug fixes and enhancements over the previous version. (BZ#706949)

Bug Fixes

BZ#695777

In the previous version of Red Hat Enterprise Linux, when an attempt to convert a negative value of a Variant Qpid type into an unsigned short type value was made, an exception was issued. In Red Hat Enterprise Linux 6, no exception was issued and the value was converted, e.g. "-5" became "65531". This bug has been fixed and the exception is now properly issued in the described scenario.

BZ#735058

Previously, non-static "isManagementMessage" class member was sometimes passed an uninitialized value. This bug has been fixed and only initialized values are now passed in the described scenario.

BZ#740912

The XML-Exchange library (as part of the qpid-cpp-server-xml package) is only available on x86, Intel 64, and AMD64 architectures. Previously, this caused additional dependencies on the xqilla and xerces-c packages to be added to the qpid-cpp RPM package. However, functionality of these two packages is not needed for the Matahari agent infrastructure. This update removes the dependency on these two packages for the PowerPC and IBM System z architectures.

Enhancement

BZ#663461

Previously, qpid-cpp was only built for x86, Intel 64, and AMD64 architectures. This update adds support, which is needed to provide the Matahari agent infrastructure on PowerPC and IBM System z architectures.

Users of qpid-cpp are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.258. QPID-QMF

4.258.1. RHBA-2011:1671 — qpid-qmf bug fix and enhancement update

Updated qpid-qmf packages that fix a bug and add various enhancements are now available for Red Hat Enterprise Linux 6.

The qpid-qmf package provides an extensible management framework layered on Qpid messaging.

The qpid-qmf package has been upgraded to upstream version 0.12, which provides a number of enhancements over the previous version. (BZ#706990)

Bug Fix

BZ#743657

Prior to this update, when "RequestContext._complete" was invoked, it would clear the Agent's context, but not the Agent's sequence manager. Consequently qmf console objects caused memory leaks. With this update the code has been corrected and the memory leak of object instances in the Python console no longer occurs.

Enhancement

BZ#699499

The qmfv2 utility did not provide a way to determine via a pollable file descriptor if a new event was available. Consequently more processor intensive methods were used. With this update a new, optional, feature has been added, "qmf_fd". It is a file descriptor that is readable if, and only if, there is at least one qmf event to be processed.

Users are advised to upgrade to these updated qpid-qmf packages, which fix this bug and adds this enhancement.

4.259. QPID-TESTS

4.259.1. RHBA-2011:1667 — qpid-tests bug fix update

An updated qpid-tests package is now available for Red Hat Enterprise Linux 6.

The qpid-tests package contains conformance tests for Apache Qpid.

The qpid-tests package has been upgraded to upstream version 0.12, which provides a number of bug fixes and enhancements over the previous version. (BZ#706991)

All users of qpid-tests are advised to upgrade to this updated package.

4.260. QPID-TOOLS

4.260.1. RHBA-2011:1668 — qpid-tools bug fix update

An updated qpid-tools package that fixes various bugs and adds an enhancement is now available for Red Hat Enterprise Linux 6.

The qpid-tools package provides management and diagnostic tools for Apache Qpid brokers and clients.

The qpid-tools package has been upgraded to upstream version 0.12, which provides a number of bug fixes and enhancements over the previous version. (BZ#706992)

Bug Fixes

BZ#688163

Prior to this update, the qmf-tool utility did not have options to select an authentication method. Consequently users could not connect to the qpid console securely. With this update the qmf-tool has been improved to allow extended command line options for selecting an authentication method. As a result command line options can now be used to select an authentication method and users can connect to the qpid console securely.

BZ#711180

Prior to this update, when attempting to stop a node in a cluster by specifying the ID number with the command "qpid-cluster -s [ID]", qpid-cluster terminated unexpectedly, the requested node was not stopped, and the error message "'NoneType' object has no attribute 'split'" was displayed. With this update qpid-tools no longer crashes and the nodes can be stopped by specifying their IDs in the scenario described.

All users of qpid-tools are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.261. QT

4.261.1. RHSA-2011:1328 — Moderate: qt security update

Updated qt packages that fix two security issues are now available for Red Hat Enterprise Linux 6 FasTrack.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. HarfBuzz is an OpenType text shaping engine.

Security Fixes

CVE-2011-3193

A buffer overflow flaw was found in the harfbuzz module in Qt. If a user loaded a specially-crafted font file with an application linked against Qt, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

CVE-2011-3194

A buffer overflow flaw was found in the way Qt handled certain gray-scale image files. If a user loaded a specially-crafted gray-scale image file with an application linked against Qt, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of Qt should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications linked against Qt libraries must be restarted for this update to take effect.

4.261.2. RHBA-2011:1170 — qt bug fix update

Updated qt packages that resolve several issues are now available for Red Hat Enterprise Linux 6.

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System.

Bug Fixes

BZ#562132

While using the Lohit font in the Malayalam script, the ra-kar character combination (0D4D + 0D30 in Unicode) was rendered incorrectly. This issue has been fixed and this combination is now rendered correctly.

BZ#679759

Example binary files in the qt-examples package were missing execute permissions, which meant that normal users could not run them. This has been fixed: file permissions have been corrected and the example files now can be executed properly.

BZ#680088

Due to an issue in the qt buildroot, the complexpong example was incorrectly removed for the PowerPC architecture qt-examples package, which caused that missing files were reported when the qt-examples file list was verified. This issue has been fixed: the complexpong example is now correctly included for all supported architectures.

BZ#716694

Previously, the /etc/rpm/macros.qt4 file was part of the qt-x11 package, which was incorrect. This issue has been corrected: the file has been moved into the qt-devel package.

All users of qt are advised to upgrade to these updated packages, which resolve these issues.

4.262. QT3

4.262.1. RHBA-2011:1269 — qt3 bug fix update

Updated qt3 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System.

Bug Fix

BZ#651426

Prior to this update, the 64-bit architecture was not preferred over the 32-bit architecture when setting the PATH environment variable on the 64-bit PowerPC platform. This bug has been fixed in this update so that the 64-bit architecture is now preferred.

All users of qt3 are advised to upgrade to these updated packages, which fix this bug.

4.263. RAPTOR

4.263.1. RHSA-2012:0410 — Important: raptor security update

Updated raptor packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

Raptor provides parsers for Resource Description Framework (RDF) files.

Security Fix

CVE-2012-0037

An XML External Entity expansion flaw was found in the way Raptor processed RDF files. If an application linked against Raptor were to open a specially-crafted RDF file, it could possibly allow a remote attacker to obtain a copy of an arbitrary local file that the user running the application had access to. A bug in the way Raptor handled external entities could cause that application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Red Hat would like to thank Timothy D. Morgan of VSR for reporting this issue.

All Raptor users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications linked against Raptor must be restarted for this update to take effect.

4.264. RDMA

4.264.1. RHEA-2011:1639 — RDMA stack bug fix and enhancement update

Updated RDMA packages that fix various bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Enterprise Linux includes a collection of InfiniBand and iWARP utilities, libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology.

The InfiniBand/iWARP/RDMA stack components have been upgraded to more recent upstream versions.

Bug Fixes

BZ#724896, BZ#724899, BZ#724900

The perftest, qperf, and srptool packages spec files erroneously limited the 32 bit Intel build to just the i386 architecture while Red Hat Enterprise Linux 6 now defaults 32 bit Intel builds to the i686 architecture. As a consequence these packages failed to build on the i686 architecture. With this update the error has been corrected and the packages build as expected.

BZ#721101

In Red Hat Enterprise Linux 6.1 changes to network functions to support multiple IP addresses on an interface were made. This caused the ifup-ib script to fail to start IPoIB interfaces depending on how the ifcfg-ib[n] (where [n] is 0 or greater) file was written. Erroneous error messages, "Error: an inet prefix is expected rather than" or "Error, some other host already uses address" were logged. With this update, the ifup-ib script has been changed to handle an array of multiple IP addresses and the error no longer occurs in the scenario described.

Enhancements

BZ#633392

This update provides support in OpenSM for Single Root I/O Virtualization (SRIOV) using SRIOV ports exposed on Mellanox SRIOV capable devices.

BZ#725106

An OpenSM update was required in order to provide SRIOV support and the update changed the names of the libraries exported by OpenSM and the rest of the InfiniBand management stack. Therefore a new package, "compat-opensm-libs", that provides a copy of the original libraries, was added to the stack to prevent this upgrade from breaking installed applications.

All RDMA users should upgrade to these updated packages which fix these bugs and add these enhancements.

4.265. RED HAT ENTERPRISE LINUX RELEASE NOTES

4.265.1. RHEA-2011:1773 — Red Hat Enterprise Linux 6.2 Release Notes

Updated packages containing the Release Notes for Red Hat Enterprise Linux 6.2 are now available.

Red Hat Enterprise Linux minor releases are an aggregation of individual enhancement, security and bug fix errata. The Red Hat Enterprise Linux 6.2 Release Notes documents the major changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications for this minor release. Detailed notes on all changes in this minor release are available in the Technical Notes.

Refer to the Online Release Notes for the most up-to-date version of the Red Hat Enterprise Linux 6.2 Release Notes:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/6.2_Release_Notes/index.html

4.265.2. RHEA-2011:1543 — Red Hat Enterprise Linux 6.2 Release Notes

Updated packages containing the Release Notes for Red Hat Enterprise Linux 6.2 are now available.

Red Hat Enterprise Linux minor releases are an aggregation of individual enhancement, security and bug fix errata. The Red Hat Enterprise Linux 6.2 Release Notes documents the major changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications for this minor release. Detailed notes on all changes in this minor release are available in the Technical Notes.

Refer to the Online Release Notes for the most up-to-date version of the Red Hat Enterprise Linux 6.2 Release Notes:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/6.2_Release_Notes/index.html

4.266. REDHAT-RELEASE

4.266.1. RHEA-2011:1743 — redhat-release enhancement update for Red Hat Enterprise Linux 6.2

An enhanced redhat-release package is now available for Red Hat Enterprise Linux 6.2.

The redhat-release package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

This updated redhat-release package reflects changes made for the release of Red Hat Enterprise Linux 6.2.

Users of Red Hat Enterprise Linux 6 are advised to upgrade to this updated redhat-release package, which adds this enhancement.

4.267. REDHAT-RPM-CONFIG

4.267.1. RHBA-2011:1748 — redhat-rpm-config bug fix update

An updated redhat-rpm-config package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The redhat-rpm-config package is used during building of RPM packages to apply various default distribution options determined by Red Hat. It also provides a few Red Hat RPM macro customizations, such as those used during the building of Driver Update packages.

Bug Fixes

BZ#642768

Previously, when building two RPM packages, where one depended on symbols in the other, the Driver Update Program (DUP) generated "Provides" and "Requires" symbols that did not match. This bug has been fixed, and these symbols are now generated correctly by DUP in the described scenario.

BZ#681884

If two kernel modules had a dependency, where one module referred to a function implemented by the other, the symbol reference was built incorrectly. As a consequence, the package that contained the module that depended on the other module, could not be installed. A patch has been provided to address this issue, and symbol references are now generated correctly in the described scenario.

Enhancement

BZ#720866

Driver Update Disks now include additional dependency information to work with later releases of Red Hat Enterprise Linux 6, in which a small change to installer behavior will impact only newly-created Driver Update Disks. Disks made previously are not affected by this update.

Users of redhat-rpm-config are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.268. RESOURCE-AGENTS

4.268.1. RHSA-2011:1580 — Low: resource-agents security, bug fix, and enhancement update

An updated resource-agents package that fixes one security issue, several bugs, and adds multiple enhancements is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The resource-agents package contains a set of scripts to interface with several services to operate in a High Availability environment for both Pacemaker and rgmanager service managers.

This update upgrades the resource-agents package to upstream version 3.9.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#707127)

Security Fix

CVE-2010-3389

It was discovered that certain resource agent scripts set the LD_LIBRARY_PATH environment variable to an insecure value containing empty path elements. A local user able to trick a user running those scripts to run them while working from an attacker-writable directory could use this flaw to escalate their privileges via a specially-crafted dynamic library.

Red Hat would like to thank Raphael Geissert for reporting this issue.

Bug Fixes

BZ#711852

When using the Sybase database and the ASEHAagent resource in the cluster.conf file, it was not possible to run more than one ASEHAagent per Sybase installation. Consequently, a second ASEHA (Sybase Adaptive Server Enterprise (ASE) with the High Availability Option) agent could not be run.

This bug has been fixed and it is now possible to use two ASEHA agents using the same Sybase installation.

BZ#693518

The s/lang scripts, which implement internal functionality for the rgmanager package, while the central_processing option is in use, were included in the wrong package. Now, the rgmanager and resource-agents packages require each other for installation to prevent problems when they are used separately.

BZ#689801

Previously, the oracledb.sh script was using the "shutdown abort" command as the first attempt to shut down a database. With this update, oracledb.sh first attempts a graceful shutdown via the "shutdown immediate" command before forcing the shutdown.

BZ#667217

Previously, when setting up a service on a cluster with a shared IP resource and an Apache resource, the generated httpd.conf file contained a bug in the line describing the shared IP address (the "Listen" line). Now, the Apache resource agent generates the "Listen" line properly.

BZ#667222

If a high-availability (HA) cluster service was defined with an Apache resource and was named with two words, such as "kickstart httpd", the service never started because it could not find a directory with the space character in its name escaped. Now, Apache resources work properly if a name contains a space as described above.

BZ#691814

When inheritance was used in the cluster.conf file, a bug in the /usr/share/cluster/nfsclient.sh file prevented it from monitoring NFS exports properly. Consequently, monitoring of NFS exports to NFS clients resulted in an endless loop. This bug has been fixed and the monitoring now works as expected.

BZ#694816

Previously, the postgres-8 resource agent did not detect when a PostgreSQL server failed to start. This bug has been fixed and postgres-8 now works as expected in the described scenario.

BZ#709400

When using the Pacemaker resource manager, the fs.sh resource agent reported an error condition, if called with the "monitor" parameter and the referenced device did not exist. Consequently, the error condition prevented the resource from being started. Now, fs.sh returns the proper response code in the described scenario, thus fixing this bug.

BZ#727643

Previously, numerous RGManager resource agents returned incorrect response codes when coupled with the Pacemaker resource manager. Now, the agents have been updated to work with Pacemaker properly.

Enhancement

BZ#678497

With this update, when the network is removed from a node using the netfs.sh resource agent, it now recovers faster than previously.

All users of resource-agents are advised to upgrade to this updated package, which corrects these issues and adds these enhancements.

4.269. RGMANAGER

4.269.1. RHBA-2011:1595 — rgmanager bug fix and enhancement update

An updated rgmanager package that fixes various bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The rgmanager package contains the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

The rgmanager package has been upgraded to upstream version 3.0.12.1, which provides a number of bug fixes and enhancements over the previous version. Note that this update requires the resource-agents package in version 3.9.2 or later. (BZ#707118)

Bug Fixes

BZ#673167

When handling failed services, the "clusvcadm -d" command now operates consistently.

BZ#690191

Exclusive prioritization now operates on service failures instead of only on node failures.

BZ#692895

The rgmanager service no longer terminates unexpectedly with a segmentation fault when a resource agent provides invalid or corrupted metadata.

BZ#709398

Reference count handling of resources with multiple instances has been corrected.

BZ#716231

An error in handling of independent subtree failures, which caused more resources to be disabled than necessary, has been fixed.

BZ#697446, BZ#741607

The rgmanager service no longer terminates unexpectedly on startup/shutdown or during service relocation.

Enhancement

BZ#723925

The rgmanager service can now be disabled in the cluster.conf configuration file.

All users of rgmanager are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.270. RHN-CLIENT-TOOLS AND YUM-RHN-PLUGIN

4.270.1. RHBA-2011:1664 — rhn-client-tools and yum-rhn-plugin bug fix update

Updated rhn-client-tools and yum-rhn-plugin packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The rhn-client-tools and yum-rhn-plugin packages provide programs and libraries that allow a system to receive software updates from Red Hat Network or Red Hat Network Satellite.

Bug Fixes

BZ#684250

Prior to this update, the order of screens in the firstboot application may have varied depending on the current locale. This update corrects the priority of the Red Hat Network module so that the order of the firstboot screens is no longer affected by the translation in use.

BZ#684913

When rhn_register fails to verify the server's SSL certificate, it terminates with a traceback. Previously, this traceback contained a misleading exception message which treated a CA certificate as an SSL certificate. The relevant exception message has now been rephrased to make sure such a traceback does not contain misleading information.

BZ#698525

Due to an error in rhnplugin, running the "yum repolist" command may have incorrectly reported previously cached channels as available. This update adapts rhnplugin to use the list of cached channels only when the user explicitly requests it (for example, by using the "--cacheonly" command line option).

BZ#700750

When used in conjunction with yum 3.2.29, rhnplugin caused the "yum clean" command to create empty directories in the current directory for every registered Red Hat Network repository. This update ensures that no directories are created when "yum clean" is executed, as expected.

BZ#701189

When building a list of cached channels, the previous version of rhnplugin failed to verify that a cachedir directory exists. This caused this list to be empty, and any subsequent "yum clean" command therefore ignored these channels. This update adapts rhnplugin to create such a directory when necessary so that the list of cached channels can be successfully created.

BZ#702084, BZ#702107

Previously, running the "rhn-channel -L" command with an incorrect username or password or as a user without permissions to administer the system in question caused it to terminate unexpectedly with a traceback. The rhn-channel utility has been corrected to display an appropriate error message in this situation.

BZ#707161

Previously, an error in rhnplugin occasionally prevented yum from displaying the download progress

for packages from Red Hat Network or Red Hat Network Satellite. This update adapts rhnplugin to set up Red Hat Network channels during the plug-in initialization, and the download progress is now displayed for all packages.

BZ#710065, BZ#714113

Prior to this update, the presence of a UTF-8 character in an error or log message caused rhnplugin to terminate unexpectedly with a traceback. Such messages are now printed as expected.

BZ#713548

Due to incompatible APIs, an attempt to run the "spacewalk-channel -L" command on a system registered with Red Hat Network Satellite failed with a traceback. This update resolves the compatibility issue and the command no longer fails in this scenario.

BZ#725496

When processing the /etc/yum/pluginconf.d/rhnplugin.conf file, the previous version of rhnplugin incorrectly ignored options in the [main] section other than "enabled" and "gpgcheck". This update ensures that this file is now processed correctly.

BZ#729468

When a machine is already registered using the Red Hat Subscription Manager tool, an attempt to register it with RHN Classic or Red Hat Network Satellite causes the rhn_register utility to display a warning message. This update rephrases this warning message for clarity.

BZ#690440

Previously, the rhn-profile-sync(8), rhn_register(8), rhnreg_ks(8), and up2date(5) manual pages incorrectly listed /etc/sysconfig/rhn/update as the common configuration file used by RHN client programs. This update adapts these manual pages to use the correct file, /etc/sysconfig/rhn/up2date.

Users of rhn-client-tools and yum-rhn-plugin should upgrade to these updated packages, which fix these bugs.

4.271. RHNLIB

4.271.1. RHBA-2011:1665 — rhnlib bug fix update

An updated rhnlib package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The rhnlib package consists of a collection of Python modules used by the Red Hat Network (RHN) software.

Bug Fixes

BZ#688095

Due to an error in the rhnlib code, network operations would have become unresponsive when an HTTP connection to Red Hat Network (RHN) or RHN Satellite became idle. The code has been modified to use timeout for HTTP connections. Network operations are now terminated after predefined time interval and can be restarted.

BZ#730744

Prior to this update, programs that used rhnlib were not able to connect to RHN or RHN Satellite

using an IPv6 address. The code has been modified to correct this issue, and rhnlib-based applications are now able to connect to RHN or RHN Satellite without any problems with IPv6 address resolution.

All users of rhnlib are advised to upgrade to this updated package, which resolves these issues.

4.272. RICCI

4.272.1. RHBA-2011:1698 — ricci bug fix and enhancement update

Updated ricci packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The ricci packages contain a daemon and a client for remote configuring and managing of clusters.

Bug Fixes

BZ#697493

Prior to this update, the ccs_sync utility could not handle IPv6 addresses. This could prevent the cluster.conf file from being distributed to nodes. The ccs_sync utility has been modified to be able to recognize and use IPv6 addresses. Now, the cluster.conf file is distributed to all nodes correctly.

BZ#718230

The ccs tool did not add or list virtual machine services correctly when using the "ccs --addresource" command. This was caused by the virtual machine resource being incorrectly added in the "resources" tag instead of the "rm" tag. This problem has been fixed and virtual machine services are now added directly in the "rm" tag when using the ccs tool.

BZ#725722

Prior to this update, the /usr/share/ccs/cluster.rng schema file did not contain definition of the "suborg" option for the fence_cisco_ucs agent. As a consequence, the cluster.conf file was not changed when adding a fencing instance definition with the "suborg" option. With this update, the cluster.rng schema has been modified to match the schema present in the cman package.

BZ#721109

Previous versions of ricci did not require the modcluster package even though it was needed for ricci to work correctly. With this update, ricci now requires modcluster to be installed.

Enhancement

BZ#696901

The ccs utility can now parse metadata in /usr/share/cluster and lists all the services and fence devices available, as well as their options.

All users of ricci are advised to upgrade to these updated ricci packages, which fix these bugs and add this enhancement.

4.273. RNG-TOOLS

4.273.1. RHEA-2011:1774 — rng-tools bug fix update

An enhanced rng-tools package that adds two enhancements is now available for Red Hat Enterprise Linux 6.

The rng-tools package contains the random number generator user space utilities, such as the rngd daemon.

Enhancements

BZ#733452

A new "-i, --ignorefail" command line option has been added to the rngd daemon. This option allows rngd to ignore repeated warning messages about failed FIPS checks.

BZ#749629

The rngd(8) manual page has been modified to include the "-i, --ignorefail" option.

All users of rng-tools are advised to upgrade to this updated package, which adds these enhancements.

4.273.2. RHEA-2011:1776 — rng-tools enhancement update

An enhanced rng-tools package that adds two enhancements is now available for Red Hat Enterprise Linux 6.

The rng-tools package contains the random number generator user space utilities, such as the rngd daemon.

Enhancements

BZ#754752

The startup script and configuration files for the rngd daemon have been added to the /etc/init.d/ and /etc/sysconfig/ directory, respectively.

All users of rng-tools are advised to upgrade to this updated package, which adds these enhancements.

4.274. RPM

4.274.1. RHSA-2012:0451 — Important: rpm security update

Updated rpm packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6; Red Hat Enterprise Linux 3 and 4 Extended Life Cycle Support; Red Hat Enterprise Linux 5.3 Long Life; and Red Hat Enterprise Linux 5.6, 6.0 and 6.1 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Security Fix

CVE-2012-0060, **CVE-2012-0061**, **CVE-2012-0815**

Multiple flaws were found in the way RPM parsed package file headers. An attacker could create a specially-crafted RPM package that, when its package header was accessed, or during package signature verification, could cause an application using the RPM library (such as the rpm command line tool, or the yum and up2date package managers) to crash or, potentially, execute arbitrary code.

Note: Although an RPM package can, by design, execute arbitrary code when installed, this issue would allow a specially-crafted RPM package to execute arbitrary code before its digital signature has been verified. Package downloads from the Red Hat Network are protected by the use of a secure HTTPS connection in addition to the RPM package signature checks.

All RPM users should upgrade to these updated packages, which contain a backported patch to correct these issues. All running applications linked against the RPM library must be restarted for this update to take effect.

4.274.2. RHBA-2011:1737 — rpm bug fix and enhancement update

Updated rpm packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The RPM Package Manager (RPM) is a powerful command line driven package management system that can install, uninstall, verify, query and update software packages.

Bug Fixes

BZ#651951

Prior to this update, RPM did not allow for self-conflicts. As a result, a package could not be installed if a conflict was added against the name of this package. With this update self-conflicts are permitted. Now, packages can be installed as expected.

BZ#674348

The rpm2cpio.sh utility was omitted when RPM switched the default compression format for the package payload to xz. As a consequence, the utility was not able to extract files. This update adds the xz support for rpm2cpio.sh and the utility now extracts files successfully.

BZ#705115

Prior to this update, when installing a package containing the same files as an already installed package, the file with the less preferred architecture was overwritten silently even if the file was not a binary. With this update, only binary files can overwrite other binary files; conflicting non-identical and non-binary files print an error message.

BZ#705993

Previously, files, that were listed in the spec file with the %defattr(-) directive, did not keep the attributes they had in the build root. With this update, the modified RPM can now keep these attributes.

BZ#707449

Prior to this update, signing packages that had already been signed with the same key could cause the entire signing process to abort. With this update, RPM is modified so that packages with identical signatures are skipped and the others are signed.

BZ#721363

Prior to this update, passing packages with a broken signature could cause the librpm library to crash. The source code has been revised and broken signatures are now rejected.

Enhancement

BZ#680889

Previously, importing GPG keys that had already been imported before could cause RPM to fail with an error message. RPM has been modified and now imports the keys successfully.

All users of RPM are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.275. RSYSLOG

4.275.1. RHBA-2011:1673 — rsyslog bug fix and enhancement update

Updated rsyslog packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The rsyslog packages provide an enhanced, multi-threaded syslog daemon that supports MySQL, syslog/TCP, RFC 3195, permitted sender list, filtering on any message part, and fine grained output format control.

Bug Fixes

BZ#661858

Previously, running rsyslog with Transport Layer Security (TLS) and TCP caused extensive memory and CPU consumption. Consequent to this, the system could become unresponsive. The source code has been modified and problems with the memory and CPU consumption no longer occur.

BZ#698705

Prior to this update, the rsyslog initscript created an invalid lock file named rsyslogd. As a consequence, rsyslog and rsyslogd did not match and the rc daemon did not stop the process when shutting down the system. With this update, the source code is modified so that the initscript creates a valid lock file.

BZ#701782

On the IBM System z and PowerPC architectures, the rsyslog daemon did not respect the configuration to send messages using TLS encryption. As a consequence, messages were sent as plain text. With this update, rsyslog is modified to send messages encrypted.

BZ#727208

Previously, the "ActionExecOnlyOnceEveryInterval" directive did not work as expected. If another message came within the time limit, the timeout got reset and would never expire. This problem has been fixed and the timeout now expires as expected.

Enhancements

BZ#618488

Previously, rsyslog did not build the omsnmp module by default. This update provides the omsnmp module so that users are able to send syslog messages over Simple Network Management Protocol (SNMP).

BZ#683537

Previously, the rsyslog daemon included /var/log/boot.log in the /etc/logrotate.d/syslog file. The rotation caused a new boot.log file to be created with zero length, while a date was appended to the old one. Eventually, after a certain number of rotations, the boot.log data got lost. With this update, rotation is no longer used for /var/log/boot.log.

BZ#702314

This update includes the new ommail module in the rsyslog package, which can be used for sending emails based on received syslog events.

BZ#737096

This update introduces the new "SpaceLFOnReceive" configuration option and the "RSYSLOG_SysklogdFileFormat" format template. These new features allow users to configure rsyslog to behave like the sysklogd daemon, which was available in previous releases.

Users are advised to upgrade to these updated rsyslog packages, which fix these bugs and add these enhancements.

4.276. RUBY

4.276.1. RHSA-2011:1581 — Low: ruby security, bug fix, and enhancement update

Updated ruby packages that fix two security issues, various bugs, and add one enhancement are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

Security Fixes

CVE-2011-3009

It was found that Ruby did not reinitialize the PRNG (pseudorandom number generator) after forking a child process. This could eventually lead to the PRNG returning the same result twice. An attacker keeping track of the values returned by one child process could use this flaw to predict the values the PRNG would return in other child processes (as long as the parent process persisted).

CVE-2011-2705

A flaw was found in the Ruby SecureRandom module. When using the SecureRandom.random_bytes class, the PRNG state was not modified after forking a child process. This could eventually lead to SecureRandom.random_bytes returning the same string more than once. An attacker keeping track of the strings returned by one child process could use this flaw to predict the strings SecureRandom.random_bytes would return in other child processes (as long as the parent process persisted).

Bug Fixes

BZ#706332

The ruby package has been upgraded to upstream point release 1.8.7-p352, which provides a number of bug fixes over the previous version.

BZ#717709

The MD5 message-digest algorithm is not a FIPS-approved algorithm. Consequently, when a Ruby script attempted to calculate an MD5 checksum in FIPS mode, the interpreter terminated unexpectedly. This bug has been fixed and an exception is now raised in the described scenario.

BZ#730287

Due to inappropriately handled line continuations in the mkconfig.rb source file, an attempt to build the ruby package resulted in unexpected termination. An upstream patch has been applied to address this issue and the ruby package can now be built properly.

BZ#674787

When the 32-bit ruby-libs library was installed on a 64-bit machine, the mkmf library failed to load various modules necessary for building Ruby-related packages. This bug has been fixed and mkmf now works properly in the described scenario.

BZ#722887

Previously, the load paths for scripts and binary modules were duplicated on the i386 architecture. Consequently, an ActiveSupport test failed. With this update, the load paths are no longer stored in duplicates on the i386 architecture.

Enhancement

BZ#673162

With this update, SystemTap probes have been added to the ruby package.

All users of ruby are advised to upgrade to these updated packages, which resolve these issues and add this enhancement.

4.276.2. RHSA-2012:0069 — Moderate: ruby security update

Updated ruby packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

Security Fix

CVE-2011-4815

A denial of service flaw was found in the implementation of associative arrays (hashes) in Ruby. An attacker able to supply a large number of inputs to a Ruby application (such as HTTP POST request parameters sent to a web application) that are used as keys when inserting data into an array could

trigger multiple hash function collisions, making array operations take an excessive amount of CPU time. To mitigate this issue, randomization has been added to the hash function to reduce the chance of an attacker successfully causing intentional collisions.

Red Hat would like to thank oCERT for reporting this issue. oCERT acknowledges Julian Wälde and Alexander Klink as the original reporters.

All users of ruby are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

4.276.3. RHBA-2012:0425 — ruby bug fix update

Updated ruby packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Ruby is an extensible, interpreted, object-oriented scripting language. It has features to process text files and to do system management tasks.

Bug Fix

BZ#799959

If a marshaled object contained multiple child objects and the call to the Marshal.load method was interrupted by a context switch, a segmentation fault could have been triggered. This was due to a thread-safety bug in the Ruby interpreter and could affect multiple packages. To prevent segmentation faults from occurring, the destination string is marked, and data tables that are identical with symbol tables are cleared.

All users of ruby are advised to upgrade to these updated packages, which fix this bug.

4.276.4. RHEA-2012:0459 — ruby enhancement update

Enhanced ruby packages are now available for Red Hat Enterprise Linux 6.

[Updated 6 Apr 2011] The text of this advisory has been updated to reflect the fact that these packages are not new in Red Hat Enterprise Linux 6.

Ruby is an interpreted scripting language for quick-and-easy object-oriented programming. It has many features to process text files and perform system management tasks, similar to Perl. It is simple, straight-forward, and extensible.

This enhancement update moves the ruby-rdoc and ruby-devel packages from the Red Hat Enterprise Linux 6 Optional channels to the Red Hat Enterprise Linux 6 base channels. This update does not make any other changes to packages. (BZ#810128)

All users who require ruby should install these enhanced packages.

4.277. S390UTILS

4.277.1. RHBA-2011:1525 — s390utils bug fix and enhancement update

Updated s390utils packages that fix multiple bugs and add multiple enhancements are now available for Red Hat Enterprise Linux 6.

The s390utils packages contain a set of utilities and daemons related to Linux for the IBM System z architecture.

Bug Fixes

BZ#746202

The **cmsfs-fuse** did not correctly update the number of records on the disk under certain conditions. This could result in an unreadable file situation when the last free data block on the disk was used. The **cmsfs-fuse** tool has been modified to update the highest record number according to the number of records written before the disk is full. The problem with unreadable files no longer occurs.

BZ#746201

Previously, FBA-512 disks could not be mounted using the **cmsfs-fuse** utility because **csmfs-fuse** expected to find the label information at a different position than it is located on FBA-512 disks. Also, the block size of the formatted FBA-512 disk can differ from the usual FBA disk block size, which is **`512 bytes`**. With this update, **cmsfs-fuse** has been modified to detect the label information of FBA-512 disks and the formatted block size is now read from the label. FBA-512 disks can now be mounted with **cmsfs-fuse** as expected.

BZ#746195

The **cmsfs-fuse** utility incorrectly calculated logical address of the data block that was to be allocated or freed. As a consequence, a write operation failed if a disk with a block size of **`512 bytes`** was larger than **`256 MB`**. With this update, **cmsfs-fuse** has been modified to calculate logical addresses correctly, and disks with a block size of 512 bytes can be written to regardless of their capacity.

BZ#745940

Under certain circumstances, **cmsfs-fuse** could incorrectly calculate the end of a file when parsing data record of a file in the *fixed record format*. As a consequence, an attempt to read such a file failed with an *I/O error*. The **cmsfs-fuse** has been modified to calculate data records and detect the end of a file correctly. Read operations on files in the fixed record format are now successful.

BZ#745939

When performing multiple subsequent write operations on a file in the *fixed record format*, **cmsfs-fuse** could, under certain circumstances, incorrectly determine the current write position. As a consequence, write operations could fail. The **cmsfs-fuse** tool now maintains, as long as a file is open for writing, a write pointer that refers to the current write position, and thus allows **`contiguous writes`** to the file in the fixed record format without any failures.

BZ#745938

The **cmsfs-fuse** utility did not reset the record length attribute after finishing a write operation. As a consequence, the next write operation failed if a disk was mounted with the **`-o big_writes`** option, which enables write operations bigger than **`4 KB`**, and the previously written record was larger than a disk block size. With this update, **cmsfs-fuse** resets the record length attribute after every write operation, and writing to a file no longer fails in the scenario described.

BZ#736397

The **`qetharp`** utility did not check the lenght of the given interface name parameter. Therefore, the **`qetharp`** command terminated with a buffer overflow when it was executed with an interface name that was longer than **`16 bytes`**. With this update, **`qetharp`** checks the length of the interface name parameter, and properly exits with the **`Error: interface name too long`** error message if the parameter is longer than it is allowed to be.

BZ#695380

Due to the redundant `free()` function call in the configuration file of **cmsfs-fuse**, the utility attempted to deallocate already freed memory. As a consequence, **cmsfs-fuse** expressed unpredictable behavior in the file type translation mode, such as a no longer accessible file system. With this update, the superfluous **free()** function call has been removed, and **cmsfs-fuse** now behaves as expected.

BZ#745936

Under certain circumstances, a file size calculation could cause the *data type overflow* situation, which resulted in a negative value. As a consequence, it was impossible to create files larger than `2 GB`. With this update, **cmsfs-fuse** has been modified to cast data type of variables, structure members and functions used in the calculation to a longer data type before calculating the file size. The **cmsfs-fuse** utility now works as expected and files larger than `2 GB` can now be created.

BZ#740302

The **lsmem** and **chmem** utilities assumed only contiguous memory blocks. Therefore, if the memory was non-contiguous and memory blocks did not follow in the presumed order, the **lsmem** utility did not show available memory that followed after a part of the physical address space that was not mapped to physical memory, a so called `memory hole`, and the **chmem** utility did not work at all. The **lsmem** and **chmem** utilities have been modified to work correctly with non-contiguous memory.

BZ#738341

The **lscss** and **lsdasd** tools did not correctly handle a situation when running on a `sysfs` device tree that was changing. If a device disappeared from the device tree while **lscss** or **lsdasd** was attempting to access attributes of the device, the tool displayed pointless error messages. With this update, the **lscss** and **lsdasd** code has been modified to suppress the related error messages. In addition, the return code of the `lscss -h` and `lsdasd -h` commands has been corrected.

BZ#738340

The **lsluns** utility did not check whether the `SCSI Generic (sg)` driver was loaded in the kernel and `sg functionality` was thus available. Therefore, **lsluns** silently failed when it was started and `sg functionality` was unavailable on the system. With this update, **lsluns** now includes the missing check and exits with an error message when it is started on the system with the `sg functionality` unavailable.

BZ#738329

The **af_iucv**(8) man page now contains previously missing information about `HiperSockets` and `HiperSocket connections`, including an explanation on how to configure a `HiperSocket device`.

BZ#736035

Previously, the **dumpconf** utility used the `DELAY_MINUTES` variable to delay restart of a system on `kernel panic`. However, users expected immediate action, therefore dumpconf has been modified to set the `DELAY_MINUTES` variable to `0` on system restart. Restart of the system with dumpconf is now triggered immediately.

BZ#732739

The `cpuplugd` daemon did not properly handle lines commented out and did not correctly match strings in its configuration file. Consequently, lines in the configuration file that were commented out could be executed, which resulted in a parsing error, and invalid variable names were sometimes not

rejected. The comment handling and string matching routines has been corrected in the code, and **cpuplugd** now behaves as expected when parsing the configuration file.

BZ#730978

When calculating a date for a timestamp, the **Perl** localtime function incorrectly returned month within a **range from 0 to 11** instead of a **range from 1 to 12**, which resulted in timestamps shifted by one month backward. To correct this problem, returned integer is incremented by one. The **zfcpdbf** now generates correct timestamps.

BZ#730370

The **lsluns --help** command incorrectly suggested using an invalid **--ports** option. This mistake has been corrected, and the **lsluns --help** now correctly displays the **--port** option.

BZ#729610

The **fdasd** utility did not distinguish between interactive and non-interactive mode. Therefore, when running the **fdasd** utility with the **--config** or **--auto** option on a device with no valid *disk label*, **fdasd** could stop with the following output:

```
no known label
Should I create a new one? (y/n)
```

Or it could fail with the following error message:

```
Disc does not contain a VOL1 label, cannot create partitions.
exiting...
```

With this update, the **fdasd** has been modified to properly check whether it should run in interactive or non-interactive mode, and it behaves accordingly.

BZ#726414

The **cpuplugd**(8) man page has been modified to correct several typos and add one missing word.

BZ#725737

Previously, the **cpuplugd** daemon did not handle a sub-string matching correctly. The daemon also used an incorrect string length when working with user-defined variables. As a consequence, the daemon returned a parsing error if a user-defined variable name matches the prefix of a pre-defined variable, or a substring of another user-defined variable. With this update, the sub-string matching has been corrected, and cpuplugd now uses correct string length in string comparing operations. Parsing errors no longer occur in the scenario described.

BZ#718745

The **cpuplugd** did not use any mechanism to prevent multiple **cpuplugd** instances from starting. As a consequence, a race between the PID file creation and a daemon startup could result in multiple cpuplugd instances running concurrently. To resolve this problem, a file locking mechanism that uses the **flock()** function has been introduced in the **cpuplugd** code. Only one instance of **cpuplugd** is now allowed to run at the same time.

BZ#718697

The **cpuplugd** had previously not implemented sanity checks regarding minimum and maximum values for valid **CPU** and memory intervals. If a configuration with incorrect intervals was used, the

daemon could not work properly, and CPU and memory could not be used optimally. With this update, **cpuplugd** now includes CPU and memory sanity checks, ensuring its efficiency.

BZ#718198

Due to a missing **ferror()** test, the **lsreipl** utility returned an error message when it attempted to read an empty **sysfs** file. With this update, the missing check has been added, and **lsreipl** no longer returns error messages when attempting to read an empty file.

BZ#713817

The **libzfcphbaapi** library was missing some event thread cleanup code in the **HBA_FreeLibrary()** function. Therefore, the **zfcp_ping** tool could terminate unexpectedly with a *segmentation fault* if no on-line adapter was discovered. The missing event thread cleanup has been added in the code using the **pthread_cancel** and **pthread_join** functions. The **zfcp_ping** tool no longer crashes under these circumstances.

BZ#711998

The s390utils-iucvterm package uses the **grep** command in its postinstall and postuninstall scripts but it was not dependent on the grep package. Therefore, error messages were displayed when installing s390utils-iucvterm. With this update, the grep package has been added as a prerequisite for s390utils-iucvterm. No error messages now occur during the package installation.

BZ#711775

When scanning for active **Logical Unit Numbers** (LUNs) without the **-a, --active** option, the **lsluns** utility filtered a scan for well known LUNs with value **0xc101000000000000** and **0x0000000000000000**, because the SCSI report luns command is sent only to these LUNs. As a consequence, the **lsluns -a** command did not show all active LUNs but only active **well known LUNs**. The **lsluns** utility has been modified to not filter LUNs when issued with the **-a** option, and it now shows all active LUNs.

BZ#705404

The **dasdinfo** utility was missing a return code and the tool always returned **exit code 0** even if an error had occured. This update adds the missing return code and the **dasdinfo** tool now returns correct return code values.

BZ#704505

The s390utils-libzfcphbaapi package did not specify the correct location of the **libzfcphbaapi.so** common library to the **/etc/hba.conf** configuration file. Therefore, s390utils-libzfcphbaapi failed to register with the **/etc/hba.conf** configuration file. With this update, the postinstall script adds the **libzfcphbaapi /usr/lib64/libzfcphbaapi-2.1.so** line to the **/etc/hba.conf** configuration file and thus registers the s390utils-libzfcphbaapi package.

BZ#700471

The **ziomon** utility used the **--output** command line option in the code, although it was referred to as the **--outfile** option in the documentation. Using the **--outfile** option as suggested by documentation thus resulted in a **ziomon** failure. With this update, **ziomon** has been modified to accept the **--outfile** command line option as documented.

BZ#700470

The **ziomon** utility did not check whether a **debugfs** file system is mounted on the **/sys/kernel/debug/** directory. Therefore, if the mount point was a different directory, **ziomon**

failed. The missing test is now included in **ziomon**, and it now works as expected: continues if a file system is mounted on the **/sys/kernel/debug/** directory, or exits with the **ziomon: Error: Debugfs not mounted on /sys/kernel/debug.** error message if a file system is mounted on a different mount point.

BZ#729981

To print parameters of the **zipl** utility for **device-mapper multipath** devices, **zipl** uses the **zipl_helper.device-mapper** script, which parses output of other programs. If any of these programs had **locale** dependent output, the script was unable to parse the output. Consequently, **zipl** terminated with the following error:

```
Script could not determine target parameters
```

To avoid this problem, the **zipl_helper.device-mapper** script has been modified to set up standard **locale** for the current process and all child processes. The problem described no longer occurs.

Enhancements

BZ#700531

The latest versions of the **Linux 2.6 scheduler** provide the same CPU optimization functionality as the **cpuplugd** daemon does, without the negative effects of **cpuplugd** operations. Therefore, the **cpuplugd** daemon is now disabled on the system by default.

BZ#694465

With this update, the cpuplugd daemon has been significantly improved:

- A set of rules used by the **cpuplugd** daemon has been improved, and cpuplugd now provides more advanced control of the **VM Resource Manager** (VMRM) **Cooperative Memory Management** (CMM) memory balloon.
- The daemon now also provides a history function, which allows an access to previous data.
- Any data from the **/proc/vmstat** and **/proc/meminfo** files can now be used in **cpuplugd** rules and user-defined variables.
- A new **cpustat.total_ticks** variable has been introduced, which simplifies user-defined CPU percentage calculations.
- The process of timestamp generation has been simplified, and a bug with wrong timestamps and intervals due to incorrect counts with microseconds, has been fixed.
- Previously, the daemon did not re-allocate and re-initialize the history data on a **SIGHUP** signal receipt. This could cause the daemon to terminate unexpectedly with a segmentation fault if the maximum history level increased. The history data is now re-allocated and re-initialized when the daemon is reloaded and maximum history level has changed.
- The daemon used a specified update interval instead of the actual time to determine the duration of the **sleep()** function and for **swap rate** calculation. This could lead to incorrect data under certain circumstances. The **cpuplugd** daemon now uses the actual time in its calculations.

BZ#632327

The **chreipl** tool has been improved and now includes the following modifications:

- Support for **`re-IPL`** from multipath devices has been added.
- Support for **`re-IPL`** from **`Named Saved System`** (NSS) has been added.
- Additional kernel parameters now can be specified for the next **`re-IPL`**.
- Support for **`auto target`**" has been added. For the ccw, fcp, and node targets, **chreipl** can automatically find the correct **`re-IPL`** target.

All users of s390utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.278. SABAYON

4.278.1. RHBA-2011:1273 — sabayon bug fix update

Updated sabayon packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Sabayon is a tool to help system administrators and users change and maintain the default behavior of the GNOME desktop. These packages contain the graphical tools which a system administrator uses to manage Sabayon profiles.

Bug Fixes

BZ#674012

Previously, when a user configured a custom panel launcher in the profile, Sabayon terminated unexpectedly while getting details of the profile. With this update, a priority level has been set up for sorting in the Details view so that Sabayon no longer crashes while getting the profile details.

BZ#654567

Previously, when a user created a file or folder on the desktop that contained an apostrophe ("") in the name, Sabayon terminated unexpectedly when saving the profile. With this update, any apostrophe characters in the name are now escaped so that Sabayon no longer crashes and properly saves the profile.

All sabayon users are advised to upgrade to these updated packages, which fix these bugs.

4.279. SAMBA

4.279.1. RHSA-2012:0465 — Critical: samba security update

Updated samba packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6; Red Hat Enterprise Linux 5.3 Long Life; and Red Hat Enterprise Linux 5.6, 6.0 and 6.1 Extended Update Support.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Security Fix

CVE-2012-1182

A flaw in the Samba suite's Perl-based DCE/RPC IDL (PIDL) compiler, used to generate code to handle RPC calls, resulted in multiple buffer overflows in Samba. A remote, unauthenticated attacker could send a specially-crafted RPC request that would cause the Samba daemon (smbd) to crash or, possibly, execute arbitrary code with the privileges of the root user.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

4.279.2. RHSA-2012:0533 — Important: samba and samba3x security update

Updated samba3x and samba packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6 respectively.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Security Fix

CVE-2012-2111

A flaw was found in the way Samba handled certain Local Security Authority (LSA) Remote Procedure Calls (RPC). An authenticated user could use this flaw to issue an RPC call that would modify the privileges database on the Samba server, allowing them to steal the ownership of files and directories that are being shared by the Samba server, and create, delete, and modify user accounts, as well as other Samba server administration tasks.

Red Hat would like to thank the Samba project for reporting this issue. Upstream acknowledges Ivano Cristofolini as the original reporter.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

4.279.3. RHBA-2011:1519 — samba bug fix update

Updated samba packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers).

BZ#713570

Previously, **Samba** did not correctly create user principal names for trusted domain users. As a result, joining **Samba** to a Windows domain using an account from a trusted domain did not work.

With this update, composing the user principal name for Kerberos authentication has been fixed so that the bug no longer occurs.

BZ#709617

Previously, printers controlled by the Common Unix Printing System (CUPS) and shared by a **Samba** server did not display the information on "location", which was controlled by the CUPS server, on Windows clients. With this update, the bug has been fixed so that the information on "location" is now correctly displayed on Windows clients.

BZ#719355

Previously, **Samba** did not correctly support clients with plain text passwords. As a result, Windows clients were unable to connect to **Samba** with plain text passwords. With this update, **Samba** support for plain text passwords has been fixed.

BZ#703393

Previously, when a paper format on a **Samba** shared printer was selected from a Windows client, this selection was not saved properly on the **Samba** server. As a result, changing printer properties had no effect. With this update, the bug has been fixed so that the printer properties are now saved, as expected.

BZ#725281

Previously, in certain environments with many users, the **pam_winbind** module stopped operating. As a result, there were failures encountered if users attempted to log in. With this update, the bug has been fixed so that **pam_winbind** now works, as expected.

BZ#741934

Previously, **Winbind** did not recover from network connection failures after an unsuccessful user authentication. As a result, **Winbind** had to be restarted for users to be able to retry the authentication process. With this update, the bug has been fixed so that users are now able to retry the authentication process without restarting **Winbind**.

BZ#709070

Previously, there were performance problems with print servers that served a large number of printers. As a result, clients had to wait a long time to be able to use printers shared on a **Samba** server. With this update, the performance problems with print servers have been fixed.

BZ#740832

If Linux clients used the Common Internet File System (CIFS) client in the kernel to mount a **Samba** share, the ***force create mode*** parameter was not honored properly. As a result, files created on a mounted **Samba** share did not properly follow the ***umask*** parameter, and files with undesired permissions were created. With this update, the bug has been fixed and no longer occurs.

BZ#743892

Previously, **Windows Internet Explorer 9** running on Microsoft Windows 7 was unable to download files onto a **Samba** share. With this update, the bug has been fixed and no longer occurs

BZ#709641

Previously, **Winbind** was not able to correctly retrieve user and group information from a Windows server. As a result, **Winbind** was unable to expose users and groups on the local system. This bug has been fixed in this update.

BZ#705123

Previously, if **Winbind** was used to provide MS-CHAPv2 authentication for **FreeRadius**, an invalid session key was used. As a result, users with MS-CHAPv2 authentication were unable to authenticate. With this update, this bug has been fixed so that MS-CHAPv2 authentication for **FreeRadius** now works as expected.

BZ#739186

Previously, certain **Samba** components logged a large number of unimportant internal messages to the system log. This bug has been fixed in this update by increasing the log level for the log messages.

BZ#737810

Previously, the net(8) man page did not document Kerberos authentication. This bug has been fixed by adding the missing documentation to the man page.

BZ#693136

If a printer driver was installed on a **Samba** server, there was a failure encountered on the Windows client. As a result, driver settings were not properly initialized and the printer did not work properly. With this update, the bug has been fixed so that the printer driver installation now works as expected.

BZ#737808

Previously, the **net** utility used for joining the Windows domains did not use the existing Kerberos credential cache. As a result, users were unable to reuse their existing tickets to join the Windows domains with Kerberos. With this update, the **net** utility has been fixed so that it now uses existing tickets from the default credential cache.

BZ#691423

When registering the Domain Name System (DNS) names, certain **Samba** utilities aborted the DNS registration if **Samba** tried to contact a disconnected DNS name server. With this update, **Samba** has been fixed so that it skips those DNS name servers that are not available on the network.

BZ#652609

Previously, the man pages for certain **Samba** components did not document that if the Windows Services for UNIX (SFU) are enabled, or if the standard RFC 2307 LDAP attributes in the Active Directory (AD) are used, primary group membership is not calculated based on the **`gidNumber`** LDAP attribute. Instead, **Winbind** uses the **`primaryGroupID`** LDAP attribute. As a result, setting the **`gidNumber`** attribute in AD has no effect for accounts if **Winbind** is used. With this update, the man pages have been updated accordingly to reflect the aforementioned limitation.

BZ#748325

Previously, extracting files from a ZIP archive failed on the Distributed File System (DFS) shares if the ***`follow symlinks = yes`*** parameter was not set. This bug has been fixed in this update so that extracting files from the ZIP archive now works as expected.

All users of samba should upgrade to these updated packages, which fix these bugs.

4.280. SBLIM-CMPI-BASE

4.280.1. RHBA-2011:1548 — sblim-cmpi-base bug fix update

An updated sblim-cmpi-base package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The sblim-cmpi-base package provides Standards Based Linux Instrumentation for Manageability (SBLIM) Common Manageability Programming Interface (CMPI) Base Providers for System-Related Common Information Model (CIM) classes.

The sblim-cmpi-base package has been upgraded to upstream version 1.6.1, which provides a number of bug fixes over the previous version. (BZ#694514)

All users of sblim-cmpi-base are advised to upgrade to this updated package, which fixes these bugs.

4.281. SBLIM-CMPI-FSVOL

4.281.1. RHBA-2011:1549 — sblim-cmpi-fsvol bug fix and enhancement update

An updated sblim-cmpi-fsvol package that fixes several bugs and provides various enhancements is now available for Red Hat Enterprise Linux 6.

The sblim-cmpi-fsvol package provides the filesystem and volume management instrumentation allowing users to obtain information about mounted and unmounted file systems by use of CIMOM technology and infrastructure.

The sblim-cmpi-fsvol package has been upgraded to upstream version 1.5.1, which includes the Linux_CSProcessor class registration fix, and provides a number of other bug fixes and enhancements over the previous version. (BZ#694506)

Bug Fix

BZ#663833

CIMOM did not collect any information about ext4 file systems because the Linux_Ext4FileSystem class was not defined. This class has been defined and information about ext4 file systems is now collected properly.

All users of sblim-cmpi-fsvol are advised to upgrade to this updated sblim-cmpi-fsvol package, which resolves these issues and adds these enhancements.

4.282. SBLIM-CMPI-NFSV3

4.282.1. RHEA-2011:1578 — sblim-cmpi-nfsv3 bug fix and enhancement update

An updated sblim-cmpi-nfsv3 package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The sblim-cmpi-nfsv3 package provides SBLIM (Standards Based Linux Instrumentation for Manageability) CMPI (Common Manageability Programming Interface) NFSv3 Providers for NFSv3 related CIM (Common Information Model) classes.

The sblim-cmpi-nfsv3 package has been upgraded to upstream version 1.1.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#694508)

All users of sblim-cmpi-nfsv3 are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.283. SBLIM-GATHER

4.283.1. RHBA-2011:1593 — sblim-gather bug fix update

Updated sblim-gather packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The sblim-gather package (Standards Based Linux Instrumentation for Manageability Performance Data Gatherer Base) contains agents and control programs for gathering and providing performance data and CIM (Common Information Model) Providers.

The sblim-gather package has been upgraded to upstream version 2.2.3, which provides a number of bug fixes over the previous version. (BZ#633991)

Bug Fixes

BZ#712043

Previously, CIM Metrics providers specific to IBM System z were missing from the sblim-gather package, preventing proper functionality of the package on that architecture. This update ensures that the CIM Metrics providers are now properly included in the IBM System z packages, with the result that full functionality is now provided.

BZ#713174

The sblim-gather-provider package is DSP1053 compliant and advertises this via the Linux_MetricRegisteredProfile class under the root/interop namespace. Prior to this update, the registration of this class and provider was missing from the package, preventing communication with the class via CIM object managers. This bug has been fixed, and now the appropriate provider for the Linux_MetricRegisteredProfile class is properly registered under the root/interop namespace.

BZ#626769

Previously, the sblim-gather init script was incorrectly placed in the /etc/init.d directory, causing difficulties during installation of the package. With this update, the init script is correctly placed in the /etc/rc.d/init.d directory, thus fixing this bug.

BZ#627919

Previously, the sblim-gather init script exit status codes were incorrect in two scenarios: when restarting a service as a non-privileged user and when passing an invalid argument. This bug has been fixed, and all exit status codes of the sblim-gather init script are now correct.

All users of sblim-gather are advised to upgrade to these updated packages, which fix these bugs.

4.284. SBLIM-SFCB

4.284.1. RHBA-2011:1547 — sblim-sfcb bug fix update

An updated sblim-sfcb package that fixes multiple bugs is now available for Red Hat Enterprise Linux 6.

Small Footprint CIM Broker (sblim-sfcb) is a Common Information Model (CIM) server conforming to the CIM Operations over the HTTP protocol. The SFCB CIM server is robust and resource-efficient, and is therefore particularly-suited for embedded and resource-constrained environments. The sblim-sfcb package supports providers written against the Common Manageability Programming Interface (CMPI).

The sblim-sfcb package has been upgraded to upstream version 1.3.11, which provides a number of bug fixes over the previous version. (BZ#633580)

Bug Fixes

BZ#618080

When using the sfcbrepos command without the "-c" option to specify the location of the CIM schema, an error message occurred. The issue was caused by using the default CIM schema location (the /usr/lib/sfcb/CIM/ directory), which does not exist on Red Hat Enterprise Linux systems. This issue has been fixed and sfcbrepos now reflects the correct CIM schema location (the /usr/share/mof/cim-current/ directory).

BZ#618081

The sfcb system group, which is used by PAM for basic authentication, was not created automatically during package installation. This issue has been fixed and the group is now created correctly.

BZ#620303

The sblim-sfcb package was compiled without the Unix domain socket local connection functionality. This issue has been fixed and this feature is now enabled in the SFCB CIM server.

BZ#745261

Due to missing checks on pointer validity when freeing memory in certain parts of the code, the SBLIM Web-Based Enterprise Management (WBEM) Command Line Interface (sblim-wbemcli) terminated unexpectedly with a segmentation fault upon successful completion of a CIM request. With this update, the missing checks have been added, pointers are now tested for NULL before an attemp to free the memory and set to NULL explicitly after the memory is freed. Segmentation faults no longer occur and sblim-wbemcli no longer crashes in the scenario described.

All users of sblim-sfcb are advised to upgrade to this updated package, which fixes these bugs.

4.285. SBLIM-SFCC

4.285.1. RHBA-2011:1583 — sblim-sfcc bug fix update

An updated sblim-sfcc package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The small footprint CIM client library (sblim-sfcc) is a C API allowing client applications to interface with CIM (Common Information Model) implementations (e.g. CIM servers). Due to its small memory and disk footprint it is well-suited for embedded environments.

The sblim-sfcc package has been upgraded to upstream version 2.2.2, which provides a number of bug fixes over the previous version. (BZ#715331)

All users of sblim-sfcc are advised to upgrade to this updated package, which fixes these bugs.

4.286. SBLIM-SMIS-HBA

4.286.1. RHBA-2011:1270 — sblim-smis-hba bug fix update

An updated sblim-smis-hba package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The sblim-smis-hba package provides SMI-S standards based HBA CMPI Providers for CIMOM technology/infrastructure.

Bug Fix

BZ#620422

Prior to this update, the sblim-smis-hba package's license field contained both the EPL and SNIA licenses, although no code in the package is licensed under the SNIA license. This bug has been fixed in this update by removing the SNIA license from the license field so that the field now contains the correct information.

All users of sblim-smis-hba are advised to upgrade to this updated package, which fixes this bug.

4.287. SCSI-TARGET-UTILS

4.287.1. RHBA-2011:1762 — scsi-target-utils bug fix and enhancement update

An updated scsi-target-utils package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The scsi-target-utils package contains the daemon and tools used to set up iSCSI and The iSCSI Extensions for RDMA (iSER) targets.

Bug Fixes

BZ#712807

Prior to this update, scsi-target-utils could under certain circumstances terminate unexpectedly with a segmentation fault when the tgt daemon was stopped. This update modifies the source code so that scsi-target-utils no longer terminates with a segmentation fault when tgtd is stopped.

BZ#736740

Prior to this update, the SCSI target configuration tool (tgt-admin) allowed only an insufficiently small number of targets to be updated. As a result, running tgt-admin with the option update ALL failed with an error message that the target already existed. With this update, tgt-admin has been modified so that it now successfully processes large numbers of targets.

Enhancement

BZ#679046

This update increases the allowable lengths of scsi_sn and scsi_id to 36 characters to allow the use of globally unique identifiers (GUID) for these properties.

All users of scsi-target-utils are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.288. SEABIOS

4.288.1. RHBA-2011:1680 — seabios bug fix update

An updated seabios package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The seabios package contains a legacy BIOS implementation which can be used as a coreboot payload.

Bug Fixes

BZ#727328

Previously, the smp_mtrr array was not large enough to hold all 31 entries of model-specific registers (MSRs) with current qemu-kvm implementations. As a consequence, installation of a Windows Server 2008 32-bit guest failed when more than one virtual CPU was allocated in it. With this update, the size of the smp_mtrr array has been increased to 32 and now Windows Server 2008 guests install successfully in the described scenario.

BZ#733028

On reboot, reinitialization of the USB HID (Human Interface Device) devices was not done before seabios was setting up timers. Consequently, when the "shutdown -r now" command was executed in a guest, the guest became unresponsive, could not be rebooted, and the "usb-kbd: warning: key event queue full" error message was returned. A patch has been provided to address this issue and the guest now reboots properly in the described scenario.

BZ#630975

Previously, seabios only supported address space up to 40 bits per one address. As a consequence, guests with 1 TB of RAM could not boot. A patch has been provided to address this issue, which raises the memory space limit up to 48 bits, thus supporting up to 281 TB of virtual memory in a guest.

BZ#736522

Previously, the S3/S4 power state capability was advertised in the DSDT (Differentiated System Description Table) tables. This could have caused various power management issues. With this update, the S3/S4 capability has been removed from the DSDT tables, thus fixing this bug.

BZ#750191

Previosly, Windows guests failed to generate memory dumps on NMIs (Non-Maskable Interrupts), even if they were properly configured to. With this update, a NMI descriptor has been added to seabios, and Windows guests now generate memory dumps on NMIs correctly.

All users of seabios are advised to upgrade to this updated package, which fixes these bugs.

4.289. SED

4.289.1. RHBA-2011:1116 — sed bug fix update

An updated sed package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The sed package provides is a stream or batch (non-interactive) editor that takes text as input, performs an operation or a set of operations on the text, and outputs the modified text.

Bug Fixes

BZ#721349

Prior to this update, the is_selinux_disabled() function was not correctly checked. With this update, this check returns the correct value and now the check works as expected.

BZ#679921

Prior to this update, the behavior of the i/--in-place option for symlinks and hardlinks was not clearly documented. With this update, the manpage and the user documentation has been improved and this problem is resolved.

All sed users are advised to upgrade to this updated package, which fixes these bugs.

4.290. SEEKWATCHER

4.290.1. RHBA-2011:1114 — seekwatcher bug fix update

An updated seekwatcher package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The seekwatcher package generates graphs from blktrace runs to help visualize I/O patterns and performance. It can plot multiple blktrace runs together, making it easy to compare the differences between different benchmark runs.

Bug Fix

BZ#681703

Prior to this update, an obsolete "matplotlib" configuration directive in seekwatcher caused seekwatcher to emit a spurious warning when executed. This bug has been fixed in this update and no longer occurs.

All users of seekwatcher should upgrade to this updated package, which fixes this bug.

4.291. SELINUX-POLICY

4.291.1. RHBA-2011:1511 — selinux-policy bug fix and enhancement update

Updated selinux-policy packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#665176

Most of the major services in Red Hat Enterprise Linux 6 have a corresponding ***service*_selinux**(8) manual page. Previously, there was no manual page for the **MySQL** service (`mysqld`). This update corrects this error, and the selinux-policy packages now provide the **mysql_selinux**(8) manual page as expected.

BZ#694031

When the SELinux Multi-Level Security (MLS) policy was enabled, running the `userdel -r` command caused Access Vector Cache (AVC) messages to be written to the audit log. With this update, the relevant policy has been corrected so that **userdel** no longer produces these messages.

BZ#698923

When SELinux was running in enforcing mode, an incorrect SELinux policy prevented the **kadmin** utility (a program for Kerberos V5 database administration) from setting process priority. With this update, the SELinux policy has been corrected, and **kadmin** now works as expected.

BZ#701885

Previously, the output of the **`semanage boolean -l`** command contained errors. This update fixes the descriptions of various SELinux Booleans to ensure the aforementioned command now produces correct output without errors.

BZ#704191

Prior to this update, the **`secadm`** SELinux user was not allowed to modify SELinux configuration files. With this update, the relevant SELinux policy has been corrected and the **`secadm`** SELinux user can now modify such configuration files as expected.

BZ#705277, BZ#712961, BZ#716973

With SELinux enabled, the **`rsyslogd`** service was previously unable to send messages encrypted with the Transport Layer Security (TLS) protocol. This update corrects the relevant SELinux policy, and **`rsyslogd`** can now send such messages as expected.

BZ#705489

With SELinux enabled, configuring cluster fencing agents to use the SSH or Telnet protocol caused these fencing agents to fail. This update contains updated SELinux rules and introduces a new **`fenced_can_ssh`** Boolean, which allows the fencing agents to use these protocols.

BZ#706086

Due to a constraint violation, when SELinux was running in enforcing mode, the **`xinetd`** service was unable to connect to **`localhost`** and the operation failed. With this update, **`xinetd`** is now trusted to write outbound packets regardless of the network's or node's Multi-Level Security (MLS) range, which resolves this issue.

BZ#706448

Due to an incorrect SELinux policy, when the user added a NIS username to the **`/etc/cgrules.conf`** configuration file, SELinux incorrectly prevented **`cgroups`** from properly applying rules to NIS users. This update corrects this error by adding an appropriate policy so that SELinux no longer prevents **`cgroups`** from applying rules to NIS users.

BZ#707616

Previously, the SELinux Multi-Level Security (MLS) policy incorrectly prevented a MLS machine form registering with Red Hat Network. This update corrects the SELinux policy so that MLS machines can now be registered as expected.

BZ#710357

Prior to this update, various incorrect SELinux labels caused several Access Vector Cache (AVC) messages to be written to the audit log. With this update, the SELinux labels that triggered these AVC messages have been corrected so that such AVC messages no longer appear in the log.

BZ#713218

Due to incorrect SELinux policy rules, the **Kerberos 5 Admin Server** (**`kadmind`**) was unable to contact the LDAP server and failed to start. This update fixes the relevant policy and **`kadmind`** now starts as expected.

BZ#714620

With SELinux running in enforcing mode, the **sssd** service did not work properly and when any user authenticated to the **sshd** service using the Generic Security Services Application Program Interface (GSSAPI), subsequent authentication attempts failed. This update adds an appropriate security file context for the **/var/cache/krb5cache/** directory, which allows **sssd** to work correctly.

BZ#715038

Previously, various labels were incorrect and rules for creating new 389-ds instances were missing. Consequent to this, when the user created a new **389-ds** instance using the **389-console** utility, several Access Vector Cache (AVC) messages appeared in the audit log. With this update, the erroneous labels have been fixed and missing rules have been added so that new **389-ds** instances are now created without these AVC messages.

BZ#718390

Due to incorrect SELinux policies, the **puppetmaster** service was not allowed to get attributes of the **chage** utility and any attempt to do so caused Access Vector Cache (AVC) messages to be written to the audit log. With this update, the SELinux policy rules have been adapted to allow **puppetmaster** to perform this operation.

BZ#719261

When SELinux was running in enforcing mode, it incorrectly prevented the **Postfix** mail transfer agent from re-sending queued email messages. This update adds a new security file context for the **/var/spool/postfix/maildrop/** directory to make sure **Postfix** is now allowed to re-send queued email messages as expected.

BZ#719929

The previous version of the **httpd_selinux**(8) manual page was incomplete and did not provide any information about the following Booleans:

- httpd_enable_ftp_server
- httpd_execmem
- httpd_read_user_content
- httpd_setrlimit
- httpd_ssi_exec
- httpd_tmp_exec
- httpd_use_cifs
- httpd_use_gpg
- httpd_use_nfs
- httpd_can_check_spam
- httpd_can_network_connect_cobbler
- httpd_can_network_connect_db
- httpd_can_network_connect_memcache

- httpd_can_network_relay
- httpd_dbus_avahi

With this update, this error no longer occurs and the aforementioned manual page now describes all available SELinux Booleans as expected.

BZ#722381

Due to the **/var/lib/squeezeboxserver/** directory having an incorrect security context, an attempt to start the **squeezeboxserver** service with SELinux running in enforcing mode failed and Access Vector Cache (AVC) messages were written to the audit log. With this update, the security context of this directory has been corrected so that SELinux no longer prevents **squeezeboxserver** from starting.

BZ#725414

When a non-**root** user (in the **unconfined_t** domain) ran the **ssh-keygen** utility and the **~/.ssh/** directory did not exist, the utility created this directory with an incorrect security context. This update adapts the relevant SELinux policy to make sure **~/.ssh/** is now created with the correct context (the **ssh_home_t** type).

BZ#726339

Prior to this update, SELinux prevented the **ip** utility from using the **sys_module** capabilities, which caused various Access Vector Cache (AVC) messages to be written to the audit log. With this update, an appropriate **dontaudit** rule has been added to make sure such messages are no longer logged.

BZ#727130

When SELinux was running in enforcing mode, an incorrect policy prevented the **grubby** utility from searching DOS file systems such as **FAT32** or **NTFS**. This update corrects the SELinux policy so that **grubby** can now work as expected.

BZ#727150

With the **omsnmp** module enabled, the latest version of the **rsyslog** daemon can send log messages as SNMP traps. This update adapts the SELinux policy to support this new functionality.

BZ#727290

Prior to this update, SELinux prevented the **lldpad** daemon from using the **sys_module** capabilities, which caused various Access Vector Cache (AVC) messages to be written to the audit log. With this update, an appropriate **dontaudit** rule has been added to make sure such messages are no longer logged.

BZ#728591

When SELinux was running in enforcing mode, **rsyslog** clients were incorrectly denied access to port **6514** (the syslog over TLS port). This update adds a new SELinux policy that allows **rsyslog** clients to connect to this port.

BZ#728699

Prior to this update, SELinux incorrectly prevented the **hddtemp** utility from listening on **localhost**. This update corrects this error, and the selinux-policy packages now provide updated SELinux rules that allow **hddtemp** to listen on **localhost** as expected.

BZ#728790

When running in enforcing mode, SELinux incorrectly prevented the new **fence_kdump** agent from binding to a port. This update adds appropriate SELinux rules to make sure this agent can bind to a port as expected.

BZ#729073

Due to an incorrect SELinux policy, an attempt to use **nice** to modify scheduling priority of the **openvpn** service failed, because SELinux prevented it. This update provides updated SELinux rules and adds a **sys_nice** capability so that users are now allowed to modify the scheduling priority as expected.

BZ#729365

The **allow_unconfined_qemu_transition** Boolean has been removed to make sure that **QEMU** is allowed to work together with the **libguestfs** library.

BZ#730218

Due to incorrect SELinux policy rules, the **procmail** mail delivery agent was not allowed to execute the **hostname** command when **HOST_NAME=`hostname`** was specified in the configuration file. This update adapts the SELinux policy to support the aforementioned **procmail** option.

BZ#730662

Prior to this update, launching a new virtual machine with a **fileinject** custom property caused Access Vector Cache (AVC) messages to be written to the audit log. With this update, the relevant SELinux policy has been corrected to ensure this action no longer produces such messages.

BZ#730837

When SELinux was running in enforcing mode, an attempt to run the **puppet** server that was configured as a Passenger web application for scaling purposes failed. This update provides adapted SELinux rules to allow this, and the **puppet** server configured as a Passenger web application no longer fails to run.

BZ#730852

When the **MAXCONN** option in the **/etc/sysconfig/memcached** configuration file was set to a value greater than **1024**, an attempt to start the **memcached** service caused Access Vector Cache (AVC) messages to be written to the audit log. This update corrects the relevant SELinux policy so that **memcached** no longer produces AVC messages in this scenario.

BZ#732196

The **git_selinux**(8) manual page now provides all information necessary to make the **Git** daemon work over the SSH protocol.

BZ#732757

When SELinux was running in enforcing mode, the Kerberos authentication for the **CUPS** web interface did not work properly. With this update, the SELinux policy has been updated to support this configuration.

BZ#733002

Most of the major services in Red Hat Enterprise Linux 6 have a corresponding ***service*_selinux**(8) manual page. Previously, there was no manual page for the **Squid** caching proxy (**squid**). This

update corrects this error, and the selinux-policy packages now provide the **squid_selinux**(8) manual page as expected.

BZ#733039

This update adds a new **abrt_selinux**(8) manual page, which explains how to configure SELinux policy for the **Automatic Bug Reporting Tool** (ABRT) service (`abrtd`).

BZ#733494

When SELinux was running in enforcing mode, the **amrecover** utility stopped responding while recovering data from a virtual tape changer. With this update, appropriate SELinux rules have been added so that **amcover** no longer hangs in this situation.

BZ#733869

Prior to this update, the **qmail-inject**, **qmail-queue**, and **sendmail** programs were not allowed to search and write into the `/var/qmail/queue/` directory. With this update, this error has been fixed and the updated SELinux rules now allow these operations.

BZ#739618

Previously, SELinux incorrectly prevented the **Chromium** and **Google Chrome** web browsers from starting due to text file relocations. With this update, an appropriate SELinux rule has been added so that SELinux no longer prevents these web browsers from starting.

BZ#739628

Due to an error in a SELinux policy, the output of the `seinfo -r` command incorrectly contained `lsassd_t`, which is not a role. This update corrects the relevant policy to make sure the aforementioned command now produces correct output.

BZ#739883

When the `DumpLocation` option in the `abrt.conf` configuration file was set to `/tmp/abrt`, restarting the `abrtd` service caused various Access Vector Cache (AVC) messages to be written to the audit log. This update corrects the relevant SELinux policy to add support for this option, and such AVC messages are no longer reported when the `abrtd` service is restarted.

BZ#740180

Previously, an incorrect SELinux policy prevented the **pwupdate** script from sending an email. This update corrects this error so that **pwupdate** is now allowed to work as expected.

BZ#734123

When SELinux was running in enforcing mode, the **virsh** utility was unable to read form the random number generator device (`/dev/random`). This update adds appropriate SELinux rules to grant **virsh** access to this device.

BZ#735198

Prior to this update, when the user used a serial console via the iLO Virtual Serial Port (VSP) and booted to single-user mode, an Access Vector Cache (AVC) message appeared and no login prompt was displayed. With this update, the SELinux policy rules have been updated to make sure the user is now able to log in as expected in this scenario.

BZ#735813

This update adds a SELinux security context for the **/etc/passwd.adjunct** file to make it possible to use this file on a Network Information Service (NIS) server.

BZ#736300

When SELinux was running in enforcing mode, the **smbcontrol** utility was unable to use the console. This update adds appropriate SELinux rules to allow **smbcontrol** to work as expected.

BZ#736388

When SELinux was running in enforcing mode, an incorrect SELinux policy prevented the **pulse** application from executing the **fos** binary file. This error has been fixed, and **pulse** can now execute the aforementioned binary file as expected.

BZ#737571

As a consequence to recent changes to the **dhcpd** daemon, the SELinux policy incorrectly prevented this daemon from setting the **setgid** and **setuid** capabilities. This update corrects the relevant SELinux policy so that **dhcpd** can now work properly.

BZ#737635

Due to an error in a SELinux policy, SELinux incorrectly prevented **luci** from starting. These selinux-policy packages provide updated SELinux rules that allow **luci** to start as expected.

BZ#737790, BZ#741271

To reflect recent changes to the **spice-vdagent** program, the SELinux policy rules have been updated so that this program can work correctly.

BZ#738156

Prior to this update, the **/etc/dhcp/dhcp6.conf** and **/etc/rc.d/init.d/dhcpcd6** files had an incorrect security context. This update corrects this error, and both **/etc/dhcp/dhcp6.conf** and **/etc/rc.d/init.d/dhcpcd6** are now labeled correctly.

BZ#738529

When the user issued the **virt-sanlock-cleanup** command, SELinux prevented the **sanlock** deamon from working properly and various Access Vector Cache (AVC) messages appeared in the audit log. With this update, an appropriate SELinux policy has been added so that **sanlock** can now work as expected.

BZ#738994

With SELinux running in enforcing mode, the **cyrus-master** process was not allowed to bind to port **tcp/119**. Since **cyrus-master** needs this port in order to run as a Network News Transfer Protocol (NNTP) server, this update fixes the relevant policy to support this configuration.

BZ#739065

The **fence_scsi.key** file that used to be located in the **/var/lib/cluster/** directory has been recently moved to **/var/run/cluster/**. This update ensures that this file retains the correct security context.

BZ#744817

Prior to this update, the **/dev/bsr*** devices were incorrectly labeled with the **device_t** type. This update changes the security context of these devices to **cpu_device_t**.

BZ#745113

The matahari package has recently renamed its binaries, which caused these files to have an incorrect security context. This update corrects this error and ensures that both binary files and init scripts now have the correct security context.

BZ#745208

When SELinux was running in enforcing mode, an attempt to use PAM Pass-through Authentication failed with an error. This update adds a relevant SELinux policy to make sure that SELinux no longer prevents PAM Pass-through Authentication from working.

BZ#746265

When SELinux was running in enforcing mode, the **sssd** service was not allowed to create, delete, or read symbolic links in the **/var/lib/sss/pipes/private/** directory. This update corrects the relevant SELinux policy rules to allow **sssd** to perform these operations.

BZ#746616, BZ#743245

The SELinux policy rules have been updated to correctly support the **SECMARK** kernel feature.

BZ#746764

Prior to this update, the **piranha-gui** service was denied access to the **/etc/sysconfig/ha/lvs.cf** file. This update corrects the SELinux policy to grant **piranha-gui** this access.

BZ#746999

Previously, SELinux prevented the **rhev-agentd** daemon from getting attributes of all available mount points. This update corrects the relevant SELinux policy so that **rhev-agentd** can gather all necessary information.

BZ#747321

Previously, SELinux prevented the **sshd** service from getting attributes of the **/root/.hushlogin** file. This update adds a new type for this file and updates its security context to make sure that **sshd** can access it as expected.

BZ#748338

Prior to this update, the **sosreport** binary run by the **ABRT** daemon did not work properly. With this update, an appropriate SELinux policy has been added so that SELinux no longer prevents **sosreport** from working properly when it is run by ABRT.

BZ#749568

When the **finger** utility attempted to access the **/var/run/nslcd/** directory, SELinux incorrectly denied this access and wrote relevant Access Vector Cache (AVC) messages to the audit log. With this update, this error has been fixed and the selinux-policy packages now provide updated SELinux policy rules that allow **finger** to access this directory, as expected.

BZ#750519

Previously, the SELinux Multi-Level Security (MLS) policy did not allow the user to attach a USB device if the **dynamic_ownership** option was enabled in the **/etc/libvirtd/qemu.conf** configuration file. This update fixes the relevant SELinux policy to make sure such a USB device can now be correctly attached in this scenario.

BZ#750934

When SELinux was running in enforcing mode and the **unconfined** module was disabled, an attempt to start the **dirsrv-admin** service failed and Access Vector Cache (AVC) messages were written to the audit log. With this update, this error has been fixed and **dirsrv-admin** now starts as expected in this situation.

Enhancements

BZ#691828

A new SELinux policy for the **sanlock** and **wdmd** services has been added to enable using these services with **libvirt** and **vdsm**.

BZ#694879

A new SELinux policy for the **subscription-manager** utility has been added.

BZ#694881

A new SELinux policy for the **corosync-notifyd** service has been added to make the service running in the **corosync_t** domain type.

BZ#705772

A new SELinux policy for **Red Hat Enterprise Virtualization** agents has been added to allow the execution of such agents.

BZ#719738

A new SELinux policy for **CTDB** services (a clustered database based on Samba's TDB) has been added.

BZ#720463

A new SELinux policy for **Zarafa** has been added.

BZ#720939

A new SELinux policy for the **drbd** service has been added.

BZ#723947, BZ#723958, BZ#723964, BZ#723977, BZ#726696, BZ#726699

New SELinux policies have been added for the following services that were previously running in the **initrc_t** domain: **pppoe-server**, **lldpad**, **fcoemon**, **cimserver**, **uuid**, and **gatherd**.

BZ#725767

A new SELinux policy for the **abrt-dump-oops** utility has been added to prevent this utility from running in the **initrc_t** domain.

BZ#729648

A new SELinux policy has been added to allow users to establish a chrooted SFTP environment over the SSH protocol.

BZ#735326

A new SELinux policy has been added to allow *IP-in-SSH* tunneling.

BZ#736623

A new SELinux Boolean, **`git_cgit_read_gitosis_content`**, has been added to allow **Gitolite** to display a list of available Git repositories.

BZ#738188

A new SELinux Boolean, **`virt_use_sanlock`**, has been added to allow the **`libvirtd`** daemon to access the **`sanlock.sock`** file.

BZ#741967

A new SELinux policy for **Clustered Samba** commands has been added.

BZ#745531

New SELinux policies for **CloudForms** services have been added.

All users of selinux-policy are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.291.2. RHBA-2011:1779 — selinux-policy bug fix update

Updated selinux-policy packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#754112

Users cron jobs were set to run in the cronjob_t domain when the SELinux MLS policy was enabled. As a consequence, users could not run their cron jobs. With this update, the relevant policy rules have been modified and users cron jobs now run in a user domain.

BZ#754465

When the auditd daemon was listening on port 60, the SELinux Multi-Level Security (MLS) policy prevented auditd from sending audit events to itself from the same system it was running on over port 61, which is possible when using the audisp-remote plugin. This update fixes the relevant policy so that this configuration now works as expected.

BZ#754802

When running the libvirt commands, such as "virsh iface-start" or "virsh iface-destroy" in SELinux enforcing mode and NetworkManager was enabled, the commands took a noticeably long time to finish successfully. With this update, the relevant policy has been added and libvirt commands now work as expected.

All users of selinux-policy are advised to upgrade to these updated packages, which resolve these issues.

4.291.3. RHBA-2011:1837 — selinux-policy bug fix update

Updated selinux-policy packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fix

BZ#761065

When running a KDE session on a virtual machine with SELinux in enforcing mode, the session was not locked as expected when the SPICE console was closed. This update adds necessary SELinux rules which ensure that the user's session is properly locked under these circumstances.

All users of selinux-policy are advised to upgrade to these updated packages, which fix this bug.

4.291.4. RHBA-2012:0123 — selinux-policy bug fix update

Updated selinux-policy packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#786088

An incorrect SELinux policy prevented the qpidd service from starting. These selinux-policy packages contain updated SELinux rules, which allow the qpidd service to be started correctly.

BZ#784783

With SELinux in enforcing mode, the ssh-keygen utility was prevented from access to various applications and thus could not be used to generate SSH keys for these programs. With this update, the "ssh_keygen_t" SELinux domain type has been implemented as unconfined, which ensures the ssh-keygen utility to work correctly.

All users of selinux-policy are advised to upgrade to these updated packages, which fix these bugs.

4.291.5. RHBA-2012:0338 — selinux-policy bug fix update

Updated selinux-policy packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fix

BZ#796423

Previously, SELinux received deny AVC messages if the dirsrv utility executed the "modutil -dbdir /etc/dirsrv/slapd-instname -fips" command to enable FIPS mode in an NSS (Network Security Service) key/cert database. This happened because the NSS_Initialize() function attempted to use prelink which uses the dirsrv_t context. With this update, prelink with the dirsrv_t context is allowed to relabel its own temporary files under these circumstances and the problem no longer occurs.

All users of selinux-policy are advised to upgrade to these updated packages, which fix this bug.

4.291.6. RHBA-2012:0364 — selinux-policy bug fix update

Updated selinux-policy packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#796331

An incorrect SELinux policy prevented the qpidd service from connecting to the AMQP (Advanced Message Queuing Protocol) port when the qpidd daemon was configured with Corosync clustering. These selinux-policy packages contain updated SELinux rules, which allow the qpidd service to be started correctly.

BZ#796585

With SELinux in enforcing mode, an OpenMPI job submitted to the parallel universe environment failed on ssh keys generation. This happened because the ssh-keygen utility was not able to read from and write to the "/var/lib/condor/" directory". With this update, a new SELinux policy has been added for the "/var/lib/condor/" directory, which allows the ssh-keygen utility to read from and write to this directory.

All users of selinux-policy are advised to upgrade to these updated packages, which fix these bugs.

4.291.7. RHBA-2013:0903 — selinux-policy bug fix update

Updated selinux-policy packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fix

BZ#966994

Previously, the mysqld_safe script was unable to execute a shell (/bin/sh) with the shell_exec_t SELinux security context. Consequently, the mysql55 and mariadb55 Software Collection packages were not working correctly. With this update, SELinux policy rules have been updated and these packages now work as expected.

Users of selinux-policy are advised to upgrade to these updated packages, which fix this bug.

4.292. SETROUBLESHOOT

4.292.1. RHBA-2011:1509 — setroubleshoot bug fix update

Updated setroubleshoot packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The setroubleshoot packages provide tools to help diagnose SELinux problems. When Access Vector Cache (AVC) messages are generated, an alert can be displayed that provides information about the problem and helps track its resolution. Alerts are user-configurable. The same tools can be run on existing log files.

Bug Fixes

BZ#541634

Prior to this update, **sealert** exited with an exit status of 0, indicating success, even though it failed to start. With this update, **sealert** returns a correct, non-zero exit status when it fails to start.

BZ#624938

Prior to this update, the **setroubleshootd** man page described an option that was not supported by the **setroubleshootd** service. This update corrects the man page content by removing the unsupported option.

BZ#625468

Previously, the combination of the **-a**/**--analyze** option with another option (for example, **sealert -a ./test-audit.log -b** caused **sealert** to not work properly. This bug has been fixed and **sealert** alerts the user that the **-a**/**--analyze** option can not be used with another option.

BZ#627668

Prior to this update, marking an AVC message as ignored using the **Ignore** button in the SETroubleshoot GUI and, consequently, reproducing that same AVC message, would not ignore that message. With this update, the underlying source code has been modified to address this issue, and ignored AVC messages no longer appear in the SETroubleshoot GUI.

BZ#630788

When SELinux produced an alert, clicking on **show** to view the alert brought up the **sealert** browser but showed no alerts. An error message was also logged in **/var/log/messages**. This was because the **/var/lib/setroubleshoot/setroubleshoot_database.xml** database contained localized content which could not be parsed. With this update, the aforementioned database no longer contains localized content, and the **sealert** browser correctly shows all alerts.

BZ#636420

Prior to this update, the **sealert -s** or **sealert -S** commands failed with a segmentation fault when LANG was set to Japanese (***LANG=ja-JP***). With this update, the underlying source code has been modified to address this issue, and the **sealert** command no longer fails on localized file analyses.

BZ#674770

Disabling IPv6 could cause AVC messages flooding regarding different confined domains asking the kernel to load the **net-pf-10** kernel module. The appropriate **setroubleshoot** plugin was updated to not display these messages when IPv6 is blacklisted. It is recommended that users disable IPv6 using the **/etc/sysctl.conf** file. In such a case, AVC messages do not appear at all.

BZ#675154

Installing the setroubleshoot* packages did not require the pygtk2-libglade, even though **sealert** and **setroubleshoot** require this package, which caused an "ImportError" exception when running the aforementioned applications. This update fixes the **setroubleshoot** spec file and adds the pygtk2-libglade dependency.

BZ#692915, BZ#721347

Previously, the setroubleshoot-server package installed the X related packages as a dependency. This update removes this dependency.

BZ#706910

Prior to this update, **setroubleshoot** used the **report** library to send problem reports to Bugzilla. To unify configuration for bug reporting, a new library (**libreport**) was created, which unifies problem reporting in all applications. With this update, **setroubleshoot** uses the new **libreport** library for

problem reporting.

BZ#730920

This update replaces the **setroubleshoot**'s dependency on report-gtk with libreport-gtk.

BZ#708437

Selecting and copying a string of text in the SEAlert GUI resulted in the full description being copied into the clipboard, rather than just the selected string. With this update, as expected, only the selected string is copied into the clipboard.

BZ#743583

Previously, an incorrect version of the setroubleshoot-plugins package was required by a the new setroubleshoot package which was released with this update.

BZ#717616

The setroubleshoot package has been upgraded to upstream version 3.0.38-2.1, which provides a number of bug fixes and enhancements over the previous version.

BZ#745777

The setroubleshoot-plugins package has been upgraded to upstream version 3.0.16-1, which provides a number of bug fixes and enhancements over the previous version.

All users of **setroubleshoot** should upgrade to these updated packages, which fix these bugs.

4.293. SETUP

4.293.1. RHBA-2011:1171 — setup bug fix and enhancement update

An updated setup package that fixes two bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The setup package contains a set of important system configuration and setup files, such as passwd, group, and profile.

Bug Fixes

BZ#691425

Bash provides the PROMPT_COMMAND environment variable containing a command that is called when a prompt is displayed. Prior to this update, the PROMPT_COMMAND variable set by a custom profile.d script was overwritten with the default value from the /etc/bashrc script file. With this update, the /etc/bashrc script file has been updated so that it now respects a user-defined PROMPT_COMMAND variable, and does not overwrite it.

BZ#703052

Prior to this update, the /etc/host.conf configuration file contained a line "order host,bind". This line is no longer used by the glibc library and is therefore redundant. With this update, this line has been removed from the host.conf file.

Enhancements

BZ#706012

The retrace-server package creates a user ID (UID) pair and a group ID (GID) pair, both with the name "retrace" and number "174". This user and group is used by the Automated Bug Reporting Tool (ABRT) retracing server. Prior to this update, the aforementioned UID/GID pairs were not reserved by the setup package so that other packages or system administrators could have accidentally assigned those values to other users and groups. With this update, the setup package now reserves these UID and GID names and numbers so that accidental conflicts with other users and groups do not happen anymore.

BZ#709599

The rhev-agent package creates a user ID (UID) pair and a group ID (GID) pair, both with the name "rhevagent" and number "175". This user and group is used by RHEV-Agent. Prior to this update, the aforementioned UID/GID pairs were not reserved by the setup package so that other packages or system administrators could have accidentally assigned those values to other users and groups. With this update, the setup package now reserves these UID and GID names and numbers so that accidental conflicts with other users and groups do not happen anymore.

BZ#715266

The trafficserver package creates a user ID (UID) pair and a group ID (GID) pair, both with the name "ats" and number "176". This user and group is used for the configuration management functions over a cluster of nodes. Prior to this update, the aforementioned UID/GID pairs were not reserved by the setup package so that other packages or system administrators could have accidentally assigned those values to other users and groups. With this update, the setup package now reserves these UID and GID names and numbers so that accidental conflicts with other users and groups do not happen anymore.

All users are advised to upgrade to this updated setup package, which fixes these bugs and adds these enhancements.

4.294. SG3_UTILS

4.294.1. RHBA-2011:1231 — sg3_utils bug fix update

Updated sg3_utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The sg3_utils packages contain a collection of tools for SCSI devices that use the Linux SCSI generic (sg) interface. It includes utilities for database copying based on "dd" syntax and semantics (the "sg_dd", "sgp_dd" and "sgm_dd" commands), INQUIRY data checking and associated pages ("sg_inq"), mode and log page checking ("sg_modes" and "sg_logs"), disk spinning ("sg_start") and self-tests ("sg_senddiag"), as well as other utilities. It also contains the rescan-scsi-bus.sh script.

Bug Fix

BZ#628553

When scanning for iSCSI devices, if no device existed with a Logical Unit Number (LUN) of "0", then the rescan-scsi-bus.sh shell script failed to detect any other devices as well. With this update, the rescan-scsi-bus.sh script detects all iSCSI devices even if there is no device with LUN of "0".

All users of sg3_utils are advised to upgrade to these updated packages, which fix this bug.

4.295. SHADOW-UTILS

4.295.1. RHBA-2011:1650 — shadow-utils bug fix and enhancement update

An updated shadow-utils package that fixes multiple bugs and adds three enhancements is now available for Red Hat Enterprise Linux 6.

The shadow-utils package includes programs for converting UNIX password files to the shadow password format, as well as tools for managing user and group accounts.

Bug Fixes

BZ#586796

Previously, the extended access control lists (ACL) on a file or directory below the /etc/skel directory were not preserved when a new user was created. As a result, the file or directory was copied but the extended ACLs that were associated with the file or directory were lost. This update preserves these extended ACLs.

BZ#667593

Previously,the switch-group (sg) command failed with a segmentation fault when using password protected groups. This update modifies the gshadow functions in shadow-utils and also uses the gshadow functions from glibc so that the sg command now handles password protected groups as expected.

BZ#672510

Previously, the new group (newgrp) command failed with a segmentation fault when using password protected groups. This update modifies the newgrp command so that the newgrp command now handles password protected groups as expected.

BZ#674878, BZ#696213

Previously, the man page for the useradd command contained misleading information about the -m option. The -m option is described correctly.

BZ#693377

Previously, the useradd command failed with a segmentation fault when the user ID (UID) range exceeded the maximum of 2147483647 (UID_MAX) accounts on a 64bit system. This update replaces the alloca() function with the malloc() function and checks the return value. Now, the useradd command operates in this range as expected.

BZ#706321

Previously, the lastlog command did not work correctly with large UIDs on 32bit system due to integer overflow. As a result, lastlog showed only users that were logged in. This update modifies the code so that lastlog now shows also users that were never logged in.

Enhancements

BZ#723921

This update is compiled with the position-independent executable (PIE) and relocation read-only (RELRO) flags which enhance the security of the system.

BZ#639900

With this update, the userdel command offers the option to delete both from the SELinux login mapping.

BZ#629277, BZ#696213

This update adds additional comments in "/etc/login.defs". These comments inform the administrator that certain configuration options are ignored in favor of the pam-cracklib module.

All users of shadow-utils are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.296. SIGAR

4.296.1. RHBA-2011:1570 — sigar and mingw32-sigar bug fix and enhancement update

Updated sigar and mingw32-sigar packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The System Information Gatherer and Reporter (SIGAR) is a library and command line tool for accessing operating system and hardware level information across multiple platforms and programming languages.

The mingw32-sigar package provides the MinGW (Minimalist GNU for Windows) sigar library.

The sigar package has been upgraded to upstream version 1.6.5, which updates sigar to use Windows device names instead of ethX names. This update also adds a number of bug fixes and enhancements over the previous version. (BZ#688184)

Bug Fix

BZ#746288

Previously, sigar could print incorrect system information on the IBM System z architecture due to a specific format for the /proc/cpuinfo file. This update ensures that the /proc/cpuinfo file is correctly parsed on all non-x86 architectures. As a result, the correct system information is now displayed.

Enhancement

BZ#663465

This update adds PowerPC and IBM System z as a dependency for the Matahari framework on the AMD64 and Intel 64 architectures.

All users of sigar and mingw32-sigar are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.297. SLAPI-NIS

4.297.1. RHBA-2011:1700 — slapi-nis bug fix update

An updated slapi-nis package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The slapi-nis package provides the NIS server plugin and the schema compatibility plugin for the 389 directory server.

Bug Fixes

BZ#694623

Prior to this update, processing an entry referred to large numbers of other entries took an excessive amount of time when the plugin was triggered and caused multiple levels of recursion loading of the ns-slapd process. This update improves the performance of slapi-nis when processing entries that refer to large numbers of other entries.

BZ#730403

Prior to this update, slapi-nis used NSPR RW locks which are not re-entrant. As a consequence, problems could arise and lead to deadlocks. With this update, POSIX-based read-write locking that synchronizes access between threads is used to avoid potential deadlocks.

All users of slapi-nis are advised to upgrade to this updated package, which fixes these bugs.

4.298. SMARTMONTOOLS

4.298.1. RHBA-2011:1201 — smartmontools bug fix update

An updated smartmontools package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The smartmontools package contains two utilities, smartctl and smartd, that enable the controlling and monitoring of Self-Monitoring, Analysis and Reporting Technology System (S.M.A.R.T.) enabled storage systems. These utilities provide advanced warning of disk degradation and failure.

Bug Fix

BZ#697867

Prior to this update, when a system event relevant to smartd happened, the following spurious error message was output if no mail address was configured:

```
smartd: internal error in MailWarning(): cfg.mailwarn->emailfreq=0
```

This unintended behavior has been fixed in this update so that the spurious error message is no longer displayed.

All smartmontools users are advised to upgrade to this updated package, which fixes this bug.

4.299. SOS

4.299.1. RHBA-2011:1536 — Low: sos security, bug fix, and enhancement update

An updated sos package that fixes one security issue, several bugs, and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with each description below.

SOS is a set of tools that gathers information about system hardware and configuration.

Security Fix

CVE-2011-4083

The **sosreport** utility incorrectly included Certificate-based Red Hat Network private entitlement keys in the resulting archive of debugging information. An attacker able to access the archive could use the keys to access Red Hat Network content available to the host. This issue did not affect users of Red Hat Network Classic.

Bug fixes

BZ#600813

In previous versions, the **yumlist `yum`** plug-in option attempted to gather the repository list, but this option was broken: running **`sosreport -k yum.yumlist=True`** returned the following error:

```
no such option "yumlist" for plugin (yum)" error
```

With this update, the **yumlist `yum`** plug-in option is usable, and instead will include the output of the **`yum list`** command, if enabled (**`sosreport -k yum.yumlist=True`**). As this operation can be slow, **yum.yumlist** is disabled by default.

BZ#682124

Previously, the **ldap** plug-in did not include the **`/etc/nslcd.conf`** file. Consequently, no **`nslcd.conf`** file was found when running **sosreport**. With this update, sos now includes **`/etc/nslcd.conf`** in its reports on systems that are using the nss-pam-ldapd nsswitch module.

BZ#683404

Due to a regression, a bug prevented the **autofs** plug-in from collecting the output of the **`/sbin/chkconfig --list autofs`** command. This update corrects the problem and the output of **`chkconfig --list autofs`** is now correctly stored in the **`sos_commands/autofs/chkconfig_--list_autofs`** file.

BZ#704383

Due to a bug, **sosreport** did not capture *Logical Volume Manager* (LVM) information (vgscan, pvscan, lvs, pvs, and vgs). This update fixes this problem and LVM information is now collected.

BZ#713449

The **sosreport** utility could return misleading command output data. This happened because the utility called the **`stdout.strip()`** function on the returned command output and the function truncated the leading and trailing whitespace characters. With this update, the function is no longer called in this situation and the returned command output is correct.

BZ#721163

Prior to this update, the **sosreport** tool did not capture the IPv6 neighbor list. With this update, the code has been modified and **sosreport** captures the neighbor list as expected.

BZ#726360

Prior to this update, the **sosreport** tool failed to gather all the relevant data from the qpidd plug-in as the **`checkenabled()`** function was looking for the qpid package. However, no such package exists. With this update, the **`checkenabled()`** function now looks for the correct qpid-tool packages and **sosreport** gathers all the relevant qpid data as expected. In addition, a much greater set of configuration files and tool output is collected in this version.

BZ#736718

The path to the external RHN **hardware.py** plug-in was incorrect. Therefore the utility failed to locate and capture data from the plug-in. With this update, the path has been corrected and the problem no longer occurs.

Enhancements

BZ#691477

USB device information provided by **lsusb**, **lsusb -v**, and **lsusb -t** commands is now collected by **sosreport** using the **hardware** plug-in.

BZ#673244

This update adds the **infiniband** plug-in to allow **sosreport** to collect information about InfiniBand devices. If the libibverbs-utils package is installed, this plug-in will be enabled and includes the output of the **ibv_devices** and **ibv_devinfo** commands in the **sosreport** debugging archive.

BZ#677124

This update adds the **iscsitarget** plug-in to allow **sosreport** to collect iSCSI target session information and configuration. If the scsi-target-utils package is installed, this plug-in will be enabled and includes the **/etc/tgt/targets.conf** file and the output of **tgtadm --lld iscsi --op show --mode target** command in the **sosreport** debugging archive.

BZ#683219

Prior to this update, the **sosreport general** plug-in excluded files larger than 15 MB when the **syslogsize** option was specified. With this update, such files are truncated to 15 MB, in such a manner as to include the latest events, and saved in the **/sosreport/sos_commands/** directory.

BZ#694813

The **general** plug-in for **sosreport** now collects information in the **/etc/init** directory.

BZ#697899

The **networking** plug-in now collects details about bridged network interfaces if present, including the output of the **brctl show** and **brctl showstp** commands.

BZ#709491

The vmware plugin now collects information from **/proc/vmmemctl**.

BZ#714293

The **sosreport** utility now captures the **/etc/rhsm/** content.

BZ#726427

The **sosreport** utility now collects the results of the **ethtool -g**, **ethtool -c**, and **ethtool -a** commands by default.

BZ#729455

The **sosreport** utility now collects the cgroups configuration data.

All users of the sos packages are advised to upgrade to these updated packages, which address these issues and add these enhancements.

4.299.2. RHBA-2012:0556 — sos bug fix and enhancement update

Updated sos packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The sos packages contain a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

Bug Fixes

BZ#800460

An error in the parsing of the "brctl" command's output caused the sosreport utility to log errors on systems with bridged network configurations. The "sosreport" command printed a Python backtrace and certain bridge configuration information was not collected from the system. This update corrects the parsing of the "brctl" command's output so that no backtrace is printed and full bridge configuration data is collected from the system.

BZ#817921

Previously, sos used a single fixed path to collect all libvirt logs in one directory. On certain releases of Red Hat Enterprise Virtualization, the libvirtd.log file could be located in the parent directory and, therefore, the libvirtd.log file was not collected on such systems. The sosreport utility now uses a wildcard character that matches both possible locations for the file. The livirtd.log file is now collected reliably on all supported versions of Red Hat Enterprise Virtualization.

Enhancement

BZ#801328

This update adds a new plug-in that is necessary to collect the requisite logs for the Gluster product. Information is collected from the files located in the /etc/glusterd/ and /var/log/glusterfs/ directories.

All users of sos are advised to upgrade to this updated package, which fixes these bugs.

4.300. SPICE-CLIENT

4.300.1. RHBA-2012:0371 — spice-client bug fix update

An updated spice-client package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The spice-client package provides the Simple Protocol for Independent Computing Environments (SPICE) client application. SPICE is a remote display protocol designed for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

Bug Fixes

BZ#771323

The SPICE client did not properly support the Xinerama extension in full screen mode on multi-screen setups. Therefore, if the user switched to full screen mode while using Xinerama, the SPICE

client windows failed to cover all physical screens used by the guest. With this update, the underlying code has been modified to provide Xinerama support and the SPICE client now behaves correctly in full screen mode.

BZ#790892

Any attempt of sound recording in the guest failed if there was another application accessing the recording device on the SPICE client startup. This update ensures that the client uses the PulseAudio sound server, which now allows multiple applications to access the recording device at the same time.

All users of spice-client are advised to upgrade to this updated package, which fixes these bugs.

4.301. SPICE-PROTOCOL

4.301.1. RHEA-2011:1629 — spice-protocol bug fix and enhancement update

An updated spice-protocol package that fixes one bug and adds several enhancements is now available for Red Hat Enterprise Linux 6.

The spice-protocol package contains header files that describe the SPICE protocol and the QXL para-virtualized graphics card. The SPICE protocol is needed to build newer versions of the spice-client and the spice-server packages.

The spice-protocol package has been upgraded to upstream version 0.8.1, which provides a number of enhancements over the previous version, including support for asynchronous guest I/O operations, support for suspending guest I/O operations, and support for changing guest volume. (BZ#723480)

Bug Fix

BZ#738262

The SPICE client failed to connect to the SPICE server on the target host after a virtual machine had been migrated to a remote machine. This happened when the migration of the virtual machine took longer than the expiration time of the SPICE ticket that was set on the target host. Without a valid password, the SPICE server refused connection from the SPICE client and the SPICE session had to be closed. To prevent this problem, support for spice semi-seamless migration has been added. Other components such as spice-client, spice-server and qemu-kvm have also been modified to support this feature. SPICE now allows the SPICE client to connect to the SPICE server on the target host at the very start of the virtual machine migration, just before the migrate monitor command is given to the qemu-kvm application. With a valid ticket on the target host, the SPICE ticket on the destination no longer expires and the SPICE client now remains open when the virtual machine migration is done.

All users of spice-protocol are advised to upgrade to this updated package, which fixes this bug and adds these enhancements.

4.302. SPICE-SERVER

4.302.1. RHBA-2011:1634 — spice-server bug fix and enhancement update

An updated spice-server package that fixes multiple bugs and adds various enhancements is now available Red Hat Enterprise Linux 6.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

The spice-server package has been rebased to upstream version 0.8.2, which fixes multiple bugs and adds multiple enhancements. (BZ#723676)

All users requiring spice-server are advised to upgrade to this updated package, which fixes these bug and adds these enhancements.

4.303. SPICE-VDAGENT

4.303.1. RHBA-2011:1577 — spice-vdagent bug fix and enhancement update

An updated spice-vdagent package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The spice-vdagent package provides a SPICE agent for Linux guests.

The spice-vdagent package has been upgraded to upstream version 0.8.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#722477)

Note: the system must be rebooted in order for these changes to take effect.

Users are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.304. SQUID

4.304.1. RHSA-2011:1791 — Moderate: squid security update

An updated squid package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Security Fix

CVE-2011-4096

An input validation flaw was found in the way Squid calculated the total number of resource records in the answer section of multiple name server responses. An attacker could use this flaw to cause Squid to crash.

Users of squid should upgrade to this updated package, which contains a backported patch to correct this issue. After installing this update, the squid service will be restarted automatically.

4.304.2. RHBA-2012:0122 — squid bug fix update

An updated squid package that fixes one bug is now available for Red Hat Enterprise Linux 6.

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Bug Fix

BZ#788449

Squid did not properly release allocated memory when generating error page contents, which caused memory leaks. Consequently, the Squid proxy server consumed a huge amount of memory within a short time period. This update fixes this memory leak and Squid no longer consumes more memory than expected.

All users of squid are advised to upgrade to this updated package, which fixes this bug. After installing this update, the squid service will be restarted automatically.

4.304.3. RHBA-2012:0470 — squid bug fix update

Updated squid packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Bug Fix

BZ#810115

Previously, Squid did not pass the ident value to a URL rewriter that was configured using the "url_rewrite_program" directive. As a consequence, the URL rewriter received the dash character ("-") as the user value instead of the correct user name. The underlying source code has been modified so that the URL rewriter now receives the correct user name in the described scenario.

All users of squid are advised to upgrade to these updated packages, which fix this bug. After installing this update, the squid service will be restarted automatically.

4.304.4. RHBA-2012:0557 — squid bug fix update

Updated squid packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Squid is a high-performance proxy caching server for web clients that supports FTP, Gopher, and HTTP data objects.

Bug Fix

BZ#815682

Squid used as a transparent proxy can only handle the HTTP protocol. Previously, when using Squid as a transparent proxy, it was possible to define a URL in which the access protocol contained the asterisk character (*) or an unknown protocol namespace URI (Uniform Resource Identifier). As a consequence, an "Invalid URL" error message was logged in the access.log file during reload time. This update ensures that "http://" is always used in transparent proxy URLs, and error message is no longer logged in this scenario.

All users of squid are advised to upgrade to these updated packages, which fix this bug.

4.305. SSSD

4.305.1. RHBA-2011:1529 — sssd bug fix and enhancement update

Updated sssd packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The sssd packages contain a set of daemons to manage access to remote directories and authentication mechanisms.

Bug Fixes

BZ#713961

When **SSSD** communicated with an **OpenLDAP** server which supported server-side password policies but did not list them in the **`supportedControl`** attribute of the server **`rootDSE`** entry, **SSSD** terminated unexpectedly with a segmentation fault. With this update, this bug has been fixed.

BZ#713438

Previously, **SSSD** relied on the **`inotify`** kernel subsystem to detect whether a Domain Name System (DNS) resolver file was changed. If **`inotify`** returned an error (for example due to resource exhaustion), **SSSD** terminated unexpectedly and network logins no longer worked. With this update, **SSSD** itself detects the failure in the described scenario and falls back to the five-second polling, fixing this bug.

BZ#726475

Previously, **SSSD** did not properly close its Pluggable Authentication Modules (PAM) sockets after an authentication attempt, which eventually resulted in process resource exhaustion and a denial of service situation. With this update, **SSSD** has been modified to fix this problem, and file descriptors are now properly released when they are no longer in use.

BZ#703624

Previously, the internal resolver of **SSSD** was set to never retry other name servers, which were read from the **`/etc/resolv.conf`** file, if the first one failed to resolve a hostname. As a result,**SSSD** switched to offline mode without asking the other configured name servers. With this update, the bug has been fixed by configuring the resolver to query all name servers so that hostname resolution correctly retries until it either queries all the configured name servers or resolves the hostname.

BZ#707282

Previously, **SSSD** incorrectly assumed that if the **`ldap_default_authtok`** option was used, the **`ldap_default_authtok_type`** option was set to **`password`** even if it was not explicitly specified in the configuration file. With this update, **`password`** has been made the default value for the **`ldap_default_authtok_type`** option, thus the bug is now fixed.

BZ#725868

Previously, certain Lightweight Directory Access Protocol (LDAP) deployments contained a group with the option **`GID=0`** set which acted like a "root" group. As a result, the operation that processed members belonging to the group with **`GID=0`** was aborted. With this update, groups with **`GID=0`** are treated as non-POSIX groups (that is groups that are containers only and not reported to clients) so that the groups are handled gracefully.

BZ#745966

Previously, if internal communication between the PAM responder and one of **SSSD**'s back ends timed out, a handling routine was invoked. Under certain circumstances, this routine could have caused a race condition which could have resulted in accessing memory that has been freed. As a result, the PAM responder terminated unexpectedly. With this update, timeout handling routine does not free the context until all operations on this context are done, thus the bug is fixed.

BZ#748924

If an error occurred in **SSSD** during the composition of a reply message to PAM, **SSSD** tried to send a reply packet to the **`pam_sss`** module even though the packet was corrupt. As a result, the **SSSD** PAM responder terminated unexpectedly. With this update, **SSSD** now detects if the response packet is already created so that in case of the error, the client will be forcibly disconnected and the **SSSD** will not crash.

BZ#746037

The Name Service Switch (NSS) responder process of **SSSD** uses an internal hash table. If **SSSD** back end was restarted and the NSS responder reconnected, the hash table was accessed but not checked for existence. As a result, under certain circumstances, nothing was stored in the hash table before the NSS responder reconnected, and the NSS responder accessed uninitialized memory and terminated unexpectedly. With this update, the hash table is now checked for existence, thus the bug is fixed.

BZ#728267

When processing group memberships for a user who was a member of a group that lacked any POSIX attributes, the loop index was incremented even for groups that were expected to be skipped. Instead of being skipped, groups without the POSIX attributes were returned with a random GID. With this update, the loop index is now only incremented for valid POSIX groups so that correct group membership is returned.

BZ#742295

When converting string values returned by LDAP, **SSSD** used conversion with an implicit number base, which led to automatically detecting the base that was expected to be used. As a result, in case the UID or GID value returned from LDAP started with zero, the number was considered octal and after the conversion, a wrong value was used. With this update, explicit 10 base is now used for conversion so that the UID and GID values are not erroneously converted anymore.

BZ#732935

Under certain circumstances, if the Simple Authentication and Security Layer (SASL) was used, libldap could have tried to canonicalize the hostname by doing a reverse lookup. As a result, the LDAP request could have been blocked. Also if the PTR record was wrong, **SSSD** was not able to authenticate to the server at all. With this update, the bug has been fixed by adding an **SSSD** configuration directive, which allows turning the canonicalization on or off. The canonicalization is off by default.

BZ#721052

After a connection was established to the server, **SSSD** never refreshed the resolved address and kept the old one until a failure occurred while communicating with the host. As a result, if a DNS record was changed, **SSSD** was not notified until the original address stopped working. With this update, the internal resolver has been switched to honor the time to live (TTL) values that are read from DNS so that the resolved names are only valid for the period specified by the TTL field in DNS. The resolver refreshes the IP address after the interval passes.

BZ#742526

Previously, **SSSD** man pages only documented that some attributes expect lists of values but the man pages did not document how are these values supposed to be separated. With this update, the missing information has been added to the man pages, thus the bug is fixed.

BZ#719089

Previously, the buffer used for the dynamic DNS update operation was not big enough to contain IPv6 addresses. As a result, only part of the address was written into DNS, which corrupted the records. With this update, a larger buffer that is able to contain all address families is now used, thus the bug is fixed.

BZ#732974

Previously, **SSSD** did not set a special path for the Kerberos replay cache files. As a result, the files were stored in the **`/var/tmp/`** directory. Because the file names are not standardized, they were not handled by the Security-Enhanced Linux (SELinux) policy correctly. As a result, when using SELinux in Enforcing mode, **SSSD** did not work with the option **`krb5_validate`** set to **`true`**. With this update, support to specify the Kerberos replay cache directory, both at compilation time and in the configuration file, has been added into **SSSD**, also a corresponding SELinux policy update has been made to accomodate the Kerberos replay cache directory, thus the bug is fixed.

BZ#709342

Previously, the parameters for a domain name and user name were swapped in debug messages. With this update, the parameters have been fixed, thus the debug messages are now correct.

BZ#726466

Previously, the host-based access control part of **SSSD** treated all its attributes as plain strings. As a result, case-insensitive comparisons of attributes (for example host group names) failed if the attributes contained UTF-8 characters. With this update, the **SSSD** host-based access control provider utilizes **`libunistring`** for performing string comparisons where applicable so that **SSSD** is able to handle UTF-8 strings in the host-based access control rules.

BZ#726438

Previously, **SSSD** did not keep a copy of the list of supported LDAP controls during the whole LDAP operation. At the same time, it used the list of controls to determine if password expiration controls were available. As a result, password expiration warnings did not function properly because **SSSD** expected that they were not available. With this update, **SSSD** always requests the expiration controls so that the password expiration warnings are now displayed, as expected.

BZ#711416

During the login process, **SSSD** could have attempted to create a **`ccache`** file for the user if the old **`ccache`** file had already expired. The SSH daemon used different processes with different UID values for different parts of the login process. As a result, if a user password expired after the user logged in, **SSSD** was unable to switch to a new **`ccache`**. With this update, **SSSD** forces removal of the old **`ccache`** if the Kerberos authentication subprocess returns a special **`PAM_NEW_AUTHTOK_REQD`** return code so that **SSSD** is able to recreate a **`ccache`** file instead of an existing (but inactive) **`ccache`** file for a user who logs in via SSH with an expired password.

BZ#728343

Previously, **SSSD** checked for an incorrect DBus return code. As a result, instead of detecting timeouts properly, the monitor process disconnected from the back-end process, which resulted in failure to be notified about back end going online, and in network performance problems. With this

update, **SSSD** checks for a correct DBus return code and improves handling of timeouts on the DBus connection, thus the mentioned problems are fixed.

BZ#709081

Previously, the **sssd** daemon package did not explicitly specify that it required the sssd-client package of the same architecture. As a result, it was difficult to specify to install both primary and secondary architecture sssd-client packages on multiarch systems. With this update, the main sssd package now requires the sssd-client package of the same architecture, thus the bug is fixed.

BZ#732010

Previously, the LDAP provider man page incorrectly suggested that if the Generic Security Services Application Program Interface (GSSAPI) authentication is used and the Kerberos realm is not specified, the system default realm is used. With this update, the man page has been fixed so that it now correctly suggests that the realm configured in the **/etc/krb5.conf** file is used in the case mentioned above.

BZ#708009

Previously, the Kerberos ticket renewal timer tasks were issued every time a back end detected the online state. This unintended behavior has been fixed in this update so that the ticket renewal tasks are now only issued as per the ***krb5_renew_interval*** parameter.

BZ#707997

The IPA provider internally constructs an LDAP URI based on what the hostname that is specified by the ***ipa_server*** parameter resolves to. Previously, when the hostname resolved to an IPv6 address, the LDAP URI routines returned an error. As a result, the IPA provider was unable to function correctly in an IPv6 environment. With this update, the IPA provider now escapes all IPv6 addresses so that they can be consumed by the LDAP routines correctly, thus the bug is fixed.

BZ#733382

If a user or group entry had multiple names and none of them matched the Relative Distinguished Name (RDN) in LDAP, an error occurred during the processing of the entry in **SSSD**'s back end. As a result, entries with multiple names, with neither of them matching the RDN, were not stored and returned by **SSSD**. With this update, the entry that matches the RDN is now returned if the RDN attribute is the same as the name attribute, thus the bug is fixed.

BZ#738621

Previously, **SSSD** did not store any alternative entry names if the name entry included the alternative entry names. As a result, entries with multiple names stored in the **SSSD** cache were not returned by **SSSD** to the NSS client if the entries were stored with different names than what the NSS client asked for. With this update, the bug has been fixed by storing name aliases in the cache in addition to the primary name.

BZ#733399

SSSD uses an internal cache to store all entities retrieved from the server. Attributes of these entities can have different names in the cache and remote server. Under certain circumstances, **SSSD** used the attribute names for the remote server instead of the names for the local cache. As a result, if non-default attribute names were used either for the group GID or name, all groups were processed and stored to the cache incorrectly, thus not returned to the NSS client. With this update, the cache attribute names are now correctly used when processing groups that are retrieved from the server, thus the bug is fixed.

BZ#733409

During the password change, password policy attributes are checked in **SSSD**. If these attributes were incomplete, **SSSD** reported this password policy error as an internal error. As a result, the log message produced in this case was confusing. With this update, an authentication error is now reported and a proper log message is displayed so that the log messages related to the password policy are no longer confusing.

BZ#737157

Prior to this update, a generic and thus not understandable error message was displayed if a user password was changed but the password policy constraints were violated. With this update, the bug has been fixed by displaying the error message that clearly states what happened.

BZ#737172

SSSD displayed a private LDAP error message because there were no special error messages available that were dedicated to error conditions indicated by the server-side password policies. As a result, a very generic, and thus not understandable error messages were printed when this error occurred. With this update, the bug has been fixed so that a clear and understandable error message is now printed when this error occurs.

BZ#738629

Previously, **SSSD** did not store alternative names in if the user or group included these alternative names. As a result, members of groups were not returned by **SSSD** if the **`member`** attribute had different value than what was determined as the primary name for that member object. With this update, **SSSD** stores all user name or group name aliases in the cache. When determining the membership structure, **SSSD** checks for aliases in addition to the primary name so that the membership structure is correctly determined and returned.

BZ#740501

The NSS responder process of **SSSD** uses an internal hash table. If the **SSSD** back end was restarted and the NSS responder reconnected, the hash table was iterated over, but elements in it were not checked for initialization. As a result, the NSS responder could have terminated unexpectedly after it was restarted due to accessing the already freed memory. With this update, all elements from the hash table are copied first and iterated over afterwards, thus the bug is fixed.

BZ#707627

Previously, the **SSSD** man page did not explicitly list the rules for encoding IPv6 addresses. The man page has been updated and the missing content added, thus the bug is fixed.

BZ#742278

Previously, the example configuration file shipped with the **SSSD** contained directives, which were inaccurate, outdated, and technically inappropriate. With this update, a new example configuration file is provided, thus the bug is fixed.

BZ#742288

SSSD stores all users and groups retrieved from the remote server in its local cache. When writing to this cache, transactions are used. If the RFC 2307bis schema was used, one transaction was used for each entity stored in the cache. As a result, the **`initgroups`** operation performed too many disk writes, thus slowing the operation down. With this update, all entities retrieved from the remote server are first stored in an internal hash table, and then only a single transaction is used to store all the groups and their memberships so that the **`initgroups`** operation is now faster, especially for users who are members of a large number of groups.

BZ#707513

Previously, **SSSD** did not correctly escape certain special characters in the user names. As a result, the **`initgroups`** and login operations failed for users whose user names contained special characters. With this update, the user names are now escaped, thus the bug is fixed.

BZ#705434

Previously, the IPA provider reported an error if the provider did not find any group memberships for a user during the **`initgroups`** operation. As a result, the **`initgroups`** operation failed. With this update, the IPA provider has been fixed so that the provider now gracefully handles users without group memberships and the **`initgroups`** operation succeeds for users who are not members of any group.

BZ#700828

When the ***`ldap_uri`*** parameter was incorrectly configured so that the hostname part was missing, **SSSD** stored NULL in the pointer, in which the hostname was saved, and used it later on for establishing a connection. As a result, **SSSD** accessed the NULL pointer and terminated unexpectedly. With this update, the URI parsing function has been changed so it aborts when it cannot parse a valid hostname from the specified URI. **SSSD** reports an error and does not crash when an invalid ***`ldap_uri`*** parameter is used in the configuration file.

BZ#743841

SSSD's components communicate using the DBus protocol. On initializing the DBus server, the DBus library is given a file name that represents a known interface. DBus creates the socket on server startup. When server shuts down, it calls a DBus cleanup function which removes the socket. If one of the components was restarted, a race condition could have caused the socket to be removed by the old component instance after the new instance was already running and connected to it. With this update, path names that contain the server process' PID are passed to DBus and a symbolic link with a known and defined path name is pointed to the path name with PID. Clients connect to the well-known symbolic link paths. When the DBus server exits, the server only removes the path name appended with PID. Clients are still connected to the same path no matter what server is the symbolic link pointed to.

BZ#699530

Previously, the **`simple`** access provider in **SSSD** required that the user primary group was available to **SSSD**. As a result, the **`simple`** access provider did not work for users whose primary group was a local group stored in the **`/etc/group`** file because **SSSD** only handles remote groups. With this update, the failure to find the user primary group in the **`simple`** access provider is no longer treated as fatal so that users with the local primary group are handled correctly by the **`simple`** access provider.

BZ#698723

Previously, **SSSD** only informed the Kerberos library about the IP address of the password-change server if the password change request was delivered via the **`pam_sss`** module. As a result, tools that communicate directly with the password-change servers (for example **kpasswd**) were unable to operate. With this update, **SSSD** always passes the IP addresses of password change servers to the Kerberos library, thus the bug is fixed.

BZ#748412

Previously, **SSSD** did not free some temporary memory in the LDAP provider. As a result, when running the **`initgroups()`** operations, **SSSD** consumed extensive amount of memory, especially for complex membership structures. With this update, the problem with the memory consumption has

been fixed.

BZ#692404

When saving group memberships, **SSSD** uses a two-pass approach: save all the groups first, and then save their members. When a group GID is outside a specified range, the group should be skipped completely. Previously, **SSSD** correctly skipped the groups that were out of range during the save groups step, but then created the groups as a side effect of the save members step. As a result, **SSSD** did not filter groups which had a GID outside the specified range. With this update, the group save operation was changed so that only members of groups, which were processed successfully, are now saved, thus the bug is fixed.

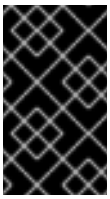
BZ#692090

Previously, **SSSD** required that all groups which **SSSD** worked with had a complete set of UNIX attributes, although the Active Directory groups can be individually set with or without the UNIX attributes. When a group without the UNIX attributes had a member with the UNIX attributes, **SSSD** did not recurse to the nested UNIX group. As a result, **SSSD** was unable to traverse the hierarchy correctly and the **`initgroups()`** operation did not return all groups correctly. With this update, **SSSD** has been changed so that it can examine non-UNIX groups for potential UNIX nested member groups. **SSSD** is now able to return the complete list of groups even if the hierarchy mixes UNIX and non-UNIX groups.

Enhancement

BZ#718250

With this update, a new option **`ipa_hbac_treat_deny_as`** has been added to **SSSD**. The default value for the option is **`DENY_ALL`**, which means that any **`DENY`** rule in the whole set of rules will deny access regardless of what is the actual rule. Alternatively, the option can be set to **`IGNORE`** to skip the **`DENY`** rules.



IMPORTANT

By ignoring the **`DENY`** rules altogether, setting the **`ipa_hbac_treat_deny_as`** option to **`IGNORE`** may, under certain circumstances, allow access to users who are not intended to be allowed.

All users of sssd should upgrade to these updated packages, which fix these bugs and add this enhancement.

4.305.2. RHBA-2012:0054 — sssd bug fix update

Updated sssd packages that fix one bug are now available for Red Hat Enterprise Linux 6.

SSSD (System Security Services Daemon) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides NSS (Name Service Switch) and PAM (Pluggable Authentication Modules) interfaces toward the system and a pluggable back end system to connect to multiple different account sources.

Bug Fix

BZ#782443

Previously, SSSD did not correctly handle LDAP authentication requests failover under a heavy load

and the request could fail with a system error. This occurred due to an invalid LDAP URI value if the second authentication request was sent before the first request could be processed by the failover service. With this update, the underlying code has been modified to ensure that the LDAP URI string remains valid until the LDAP authentication request is processed.

All users of sssd are advised to upgrade to these updated packages, which fix this bug.

4.305.3. RHEA-2011:1810 — sssd bug fix update

Updated sssd packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

SSSD provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides NSS (Name Service Switch) and PAM (Pluggable Authentication Modules) interfaces toward the system and a pluggable back end system to connect to multiple different account sources.

Bug Fixes

BZ#758696

SSSD responders did not verify whether a username string, which was passed to SSSD by a client application, contained any invalid UTF-8 characters. As a consequence, SSSD terminated unexpectedly when trying to pass such a string to the data provider over the D-Bus protocol, and the validation test performed by the libdbus library failed. To prevent this problem from occurring, UTF-8 validity checks on the string have been added in the underlying SSSD code. SSSD now does not accept username strings that are not compliant with UTF-8 encoding so that SSSD no longer crashes.

BZ#758713

When establishing a connection to an LDAP server, SSSD did not handle all possible error codes it could receive but only the ETIMEDOUT error code. Therefore, if SSSD received an error code different from ETIMEDOUT, it did not perform the expected failover to another LDAP server and switched to off-line mode. With this update, SSSD has been modified to handle all error codes received on connection attempt. SSSD now tries to connect to all specified LDAP servers and goes off-line only when it fails to connect to all of them.

All users of sssd are advised to upgrade to these updated packages, which fix these bugs.

4.306. STAR

4.306.1. RHBA-2011:0932 — star bug fix update

An updated star package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The star utility is a tape- and disk-archiving tool similar to tar that supports saving Access Control List (ACLs) permission information.

Bug Fix

BZ#611402

Under certain circumstances, the star utility could have terminated unexpectedly with a segmentation fault when used with a file which name was exactly 100 characters long. This segmentation fault has been fixed in this update and no longer occurs.

All users of star are advised to upgrade to this updated package, which fixes this bug.

4.307. STRACE

4.307.1. RHBA-2012:0028 — strace bug fix update

An updated strace package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The strace program intercepts and records the system calls called and received by a running process. It can print a record of each system call, its arguments and its return value. The strace utility is useful for diagnosing, debugging and instructional purposes.

Bug Fix

BZ#772569

The strace utility did not properly track switches between 32-bit and 64-bit process execution domains (so called "personalities") when tracing multiple processes with multiple "personalities". This caused strace to output the wrong system call names and arguments for the traced processes. This update corrects personality tracking in strace so that it now prints system call names and arguments as expected.

All users of strace are advised to upgrade to this updated package, which fixes this bug.

4.308. SUBSCRIPTION-MANAGER

4.308.1. RHBA-2011:1695 — subscription-manager bug fix and enhancement update

Updated subscription-manager packages that fix several bugs and adds an enhancement are now available for Red Hat Enterprise Linux 6.

The Subscription Manager tool allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

Bug Fixes

BZ#709412

Two variations were used in the ProductName parameter for the workstation subscription: "Red Hat Enterprise Linux Workstation" and "Red Hat Enterprise Linux 6 Workstation". As a consequence, users running the "subscription-manager list --installed" command, while subscribed to the "Red Hat Enterprise Linux Workstation" subscription, got a misleading report. With this update, the ProductId parameter is used instead to compare subscriptions in the described scenario and the bug no longer occurs.

BZ#701425

Previously, the NSS (Network Security Services) library used the "first" entitlement certificate to access all content. As a consequence, access to subsequent repositories was rejected because NSS was using the certificate from the first repository. This update allows all repositories to be controlled by unique entitlement certificates.

BZ#703921

Previously, the "Start Date" and "End Date" fields in the Contract Selection dialog window of the subscription-manager-gui utility were not populated. With this update, the dates are displayed as expected.

BZ#711133

When the subscription-manager utility had been upgraded, it put incorrect data to the sslclientkey repository parameter value. Consequently, when the yum utility was launched to install software, yum terminated with the "[Errno 14] problem with the local client certificate" error message. The bug in subscription-manager has been fixed and yum can now be run without any certificate errors.

BZ#693709

Previously, running the firstboot utility with the "-r" option while the subscription-manager-firstboot utility was already installed caused the firstboot utility to terminate with a traceback; it also failed to display a message stating that the computer was already registered with Red Hat Network. This bug has been fixed, the firstboot utility now displays the warning message properly, and no tracebacks are returned in the described scenario.

BZ#730018

When a machine was registered via the Red Hat Subscription Manager tool, an attempt to register it with Red Hat Network Classic or Red Hat Network Satellite caused the rhn_register utility to display a confusing warning message. This update rephrases this warning message for clarity.

BZ#725535

Due to a bug, the code assumed it could access the /var/rhn/rhsm directory. Consequently, the background job, which warns the user that a machine is not covered by a subscription, terminated unexpectedly if the /var/rhn/rhsm directory did not exist. With this update, the error is properly logged and the crashes no longer occur in the described scenario.

BZ#580905

The initial subscription-manager package did not provide a help function built into the user interface. Help was only available via manual pages and online documentation. This update adds a standard help button to the subscription-manager user interface.

BZ#701315

Subscriptions are represented by numeric serial numbers. When a number longer than four bytes was used as a serial number, the subscription-manager utility terminated unexpectedly. This bug has been fixed and large numbers are now supported as serial numbers in subscription-manager.

Enhancement

BZ#710172

Previously, in order to locate subscriptions for machines not covered by a subscription, a user had to log into each such machine and locate new subscriptions manually. This update allows a machine to automatically look for new subscriptions in the described scenario.

Users of subscription-manager are advised to upgrade to these updated packages, which fix these bugs.

4.308.2. RHBA-2012:0562 — subscription-manager bug fix update

Updated subscription-manager packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The subscription-manager packages provide programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat Entitlement platform.

Bug Fix

BZ#812446

Previously, the subscription-manager utility could incorrectly delete a product certificate when running the yum utility and no yum repositories were enabled or in use (for example on newly installed Red Hat Enterprise Linux 6 systems). To prevent undesirable deletions of product certificates, subscription-manager now performs a verification check before deleting a certificate. In addition, all deletions of product certificates are now logged.

All users of subscription-manager are advised to upgrade to these updated packages, which fix this bug.

4.309. SUDO

4.309.1. RHBA-2011:1175 — sudo bug fix and enhancement update

An updated sudo package that fixes one bug and introduces one feature enhancement is now available for Red Hat Enterprise Linux 6.

The sudo utility allows system administrators to give certain users the ability to run commands as root with logging.

Bug Fix

BZ#709235

Prior to this update, sudo incorrectly searched for the Lightweight Directory Access Protocol (LDAP) configuration in the /etc/nss_ldap.conf file. This bug has been fixed in this update so that sudo now searches the /etc/nslcd.conf file.

Enhancement

BZ#709859

Because the sudo utility needs to be run with elevated privileges, the sudo package is now built with RELRO linker flags.

All users of sudo are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.309.2. RHBA-2012:0565 — sudo bug fix update

Updated sudo packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root.

Bug Fixes

BZ#802440

A race condition in the signal handling code caused the sudo process to become unresponsive after receiving the SIGCHLD signal. This update modifies the signal handling to prevent the race condition, which ensures that the sudo process no longer hangs under these circumstances.

BZ#811879

The "-l" option is used to list allowed and forbidden commands for the invoking user or for the user specified by the "-U" option. However, previously, the getgrouplist() function incorrectly checked the invoker's group membership instead of the membership of the specified user. Consequently, using the "sudo" command with both the "-l" and "-U" options listed privileges granted to any group the invoker was a member of. The getgrouplist() function has been fixed to properly check the group membership of the intended user rather than checking the invoker's membership. This ensures that the required output is listed when using the "-l" and "-U options.

All users of sudo are advised to upgrade to these updated packages, which fix these bugs.

4.310. SWIG

4.310.1. RHBA-2011:0933 — swig bug fix update

An updated swig package that fixes one bug is now available for Red Hat Enterprise Linux 6.

Simplified Wrapper and Interface Generator (SWIG) is a software development utility for connecting C, C++ and Objective C programs with a variety of high-level programming languages. SWIG is primarily used with Perl, Python and Tcl/TK, but it has also been extended to Java, Eiffel and Guile. SWIG is normally used to create high-level interpreted programming environments, systems integration, and as a tool for building user interfaces.

Bug Fix

BZ#679713

Prior to this update, the swig utility emitted a nonexistent "zend_error_noreturn" function call instead of the "zend_error" call into a generated PHP code. This bug has been fixed in this update, and swig now correctly emits only the "zend_error" call as expected.

All users of swig are advised to upgrade to this updated package, which fixes this bug.

4.311. SYSTEM-CONFIG-FIREWALL

4.311.1. RHBA-2011:1223 — system-config-firewall bug fix update

Updated system-config-firewall packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The system-config-firewall packages contain a graphical user interface for basic firewall setup.

Bug Fixes

BZ#565625

Prior to this update, remote virtual machine management with TLS encryption used the same port as the one used for the unencrypted connection. With this update, the port for the remote virtual machine

management has been changed so that remote virtual machine management with TLS encryption now works as expected.

BZ#624400

Prior to this update, the Tamil translation was incomplete. As a result, certain messages were displayed in English. With this update, the missing messages have been added to the translation.

BZ#632979

Prior to this update, the Hindi translation was incomplete. As a result, certain messages were displayed in English. With this update, the missing messages have been added to the translation.

BZ#635245

Prior to this update, the Punjabi translation was incomplete. As a result, certain messages were displayed in English. With this update, the missing messages have been added to the translation.

All users of system-config-firewall are advised to upgrade to these updated packages, which fix these bugs.

4.312. SYSTEM-CONFIG-KICKSTART

4.312.1. RHBA-2011:1683 — system-config-kickstart bug fix update

An updated system-config-kickstart package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The system-config-kickstart package contains Kickstart Configurator, a graphical tool for creating kickstart files.

Bug Fix

BZ#676338

The system-config-kickstart utility terminated with a traceback if it was executed outside of a graphical environment. This problem has been fixed: the utility starts correctly in a graphical environment or displays an error message if the X Window System is not running.

All users of system-config-kickstart are advised to upgrade to this updated package, which resolves this bug.

4.313. SYSTEM-CONFIG-LVM

4.313.1. RHBA-2011:1710 — system-config-lvm bug fix update

An updated system-config-lvm package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The system-config-lvm package contains a utility for configuring logical volumes using a graphical user interface.

Bug Fix

BZ#722895

The system-config-lvm utility incorrectly left mount information in the /etc/fstab configuration file for a logical volume that had been completely removed from the system. This could have caused the system to enter single-user mode after rebooting because it was unable to mount a logical volume in /etc/fstab that no longer existed. This update ensures that system-config-lvm correctly removes the fstab entry for any logical volume that is removed.

All users of system-config-lvm are advised to upgrade to this updated package, which fixes this bug.

4.314. SYSTEM-CONFIG-PRINTER

4.314.1. RHBA-2011:1638 — system-config-printer bug fix update

Updated system-config-printer packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The system-config-printer package contains a print queue configuration tool with a graphical user interface.

Bug Fixes

BZ#556548

Previously, when a printer queue was added, CUPS (Common Unix Printing System) could leave a symbolic link in the /tmp directory. With this update, CUPS is modified to clean this data.

BZ#579864

Prior to this update, the probe_printer.py file contained a typo. As a consequence, the system-config-printer utility could terminate with a traceback if authentication was required for a CIFS (Common Internet File System) share. The typo has been corrected and tracebacks no longer occur.

BZ#591633

Prior to this update, the default firewall could prevent discovery of Multicast DNS (mDNS) devices. As a consequence, a device could not be found over the network. With this update, system-config-printer uses the D-Bus API of the system-config-firewall utility, which adjusts the firewall so that it allows network printer discovery.

BZ#608070

Due to a bug in the source code, the system-config-printer utility could terminate unexpectedly with an error message on 32-bit architectures. This problem occurred when the user changed the number of copies on the Job Options page, then pressed the Reset button to return the number of copies back to 1, and applied the changes. With this update, the system-config-printer utility is now modified and no longer terminates.

BZ#613708

Previously, only the system-config-printer base package contained the COPYING file. With this update, the COPYING file is also included in the system-config-printer-libs sub-package.

BZ#633595

Prior to this update, Korean characters were not aligned properly in certain dialog boxes. This update corrects the alignment of Korean characters.

BZ#634252

Previously, the system-config-printer utility could become unresponsive if the user provided an empty or wrong credential on a password request and closed the "Not authorized" dialog box. With this update, a D-Bus timeout is set. A new printer window now appears if the user closes the "Not authorized" dialog box.

BZ#634436

Prior to this update, multiple strings were not translated in various translations. With this update, these texts are now translated.

BZ#636523

When renaming a printer queue with a name different only in the case of some characters (lowercase/uppercase), the printer queue was deleted instead of being renamed. With this update, this type of renaming is not allowed, which prevents the queue from being unexpectedly deleted.

BZ#639624

Previously, the getJockeyDriver_thread() call tried to use D-Bus from a separate thread. As a consequence, system-config-printer could terminate unexpectedly with a segmentation fault. With this update, an error message informs users that Jockey drivers cannot be used.

BZ#645426

Prior to this update, the system-config-printer-applet could repeatedly query the CUPS scheduler for printers and jobs. As a consequence, the applet would cause high CPU consumption. With this update, system-config-printer-applet is modified and does not cause high CPU consumption any longer.

BZ#676339, BZ#676343

When executing the system-config-printer and system-config-printer-applet utilities in a non-graphical environment using the Secure Shell (SSH) connection, the utilities failed with a traceback. With this update, the utilities are now modified to provide an error message instead of a traceback.

All users of system-config-printer are advised to upgrade to these updated packages, which fix these bugs.

4.315. SYSTEM-SWITCH-JAVA

4.315.1. RHBA-2011:1744 — system-switch-java bug fix update

An updated system-switch-java package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The system-switch-java package provides a tool that allows you to select the Java environment from the list of the installed Java alternatives. The tool supports graphical user interface (GUI) and text user interface (TUI) mode.

Bug Fixes

BZ#725718

When switching to OpenJDK, the system-switch-java utility failed to switch the web plug-in to the IcedTea plug-in. This happened because system-switch-java was looking for the plug-in in a wrong location. With this update, system-switch-java searches for the web plug-in in the correct location

(/usr/lib/IcedTeaPlugin.so) and the plug-in is applied when requested.

BZ#745457

On system-switch-java 1.1.5, the command "system-switch-java --version" printed the value "1.1.4". The underlying code has been updated and the command now returns the correct version number.

All users of system-switch-java are advised to upgrade to this updated package, which fixes these bugs.

4.316. SYSTEMTAP

4.316.1. RHSA-2012:0376 — Moderate: systemtap security update

Updated systemtap packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

SystemTap is an instrumentation system for systems running the Linux kernel. The system allows developers to write scripts to collect data on the operation of the system.

Security Fix

CVE-2012-0875

An invalid pointer read flaw was found in the way SystemTap handled malformed debugging information in DWARF format. When SystemTap unprivileged mode was enabled, an unprivileged user in the stapusr group could use this flaw to crash the system or, potentially, read arbitrary kernel memory. Additionally, a privileged user (root, or a member of the stapdev group) could trigger this flaw when tricked into instrumenting a specially-crafted ELF binary, even when unprivileged mode was not enabled.

SystemTap users should upgrade to these updated packages, which contain a backported patch to correct this issue.

4.316.2. RHBA-2011:1517 — systemtap bug fix and enhancement update

Updated systemtap packages that fix several bugs and adds various enhancements are now available for Red Hat Enterprise Linux 6.

SystemTap is a tracing and probing tool that allows users to study and monitor the activities of the operating system (particularly, the kernel). It provides information similar to the output of tools like netstat, ps, top, and iostat; however, SystemTap provides more filtering and analysis options.

BZ#683483

The systemtap package has been upgraded to upstream version 1.6, which provides a number of bug fixes and enhancements:

- SystemTap now handles kernel modules with "-" in the name such as "i2c-core" properly.
- The process().mark() function now supports the $$parms log parameter for reading probe parameters.

- The operation of the compile-server and client was improved and simplified:
  - The compile server can cache the script build results.
  - The compile server and client communicate exchange version info to adjust the communication protocol and use the newest version of the compile server.
  - The following deprecated tools were removed: stap-client, stap-authorize-server-cert, stap-authorize-signing-cert, stap-find-or-start-server, and stap-find-servers.
- For remote execution, the "--remote USER@HOST" functionality can now be specified multiple times, and will automatically build the script for distinct kernel and architecture configurations and run it on all named machines at once.
- The staprun program allows to run multiple instances of the same script at the same time.

Bug Fixes

BZ#711757

When the system ran out of memory in a module, SystemTap failed to remove the module directory created by the debugfs debugger. Consequently, SystemTap was unable to load the module until after a system reboot and a kernel panic could occur. With this update, SystemTap removes the module directory properly.

BZ#708255

The rate of error or warning messages, sent from the probe module to user-space, caused various buffer overflows under certain circumstances. As a result, the messages could be lost and caused a kernel panic. With this update, these messages are also delivered if there is an excessive amount of warning or error messages.

BZ#732346

SystemTap uses the make command to search for available tracepoints ('kernel.trace("*")'). Previously, the make operation printed out a number of misleading error messages on the first tracepoint search. Because search results are cached, the error messages were produced only on the first search. With this update, the tracepoint search uses the "make -i" (ignore errors) operation, the error messages from the make operations are supressed, and no misleading output is printed when performing tracepoint searches.

BZ#737095

Prior to this update, starting a SystemTap server could fail. This occurred because the getlogin() function returned a NULL pointer when initializing an std::string object. With this update, the underlying code has been modified and the problem no longer occurs.

BZ#692970

The sdt.c tests in the testsuite were attempting to include the unavailable sdt_types.h header file, and the compilation of the systemtap-testsuite package failed. With this update, the sdt.c tests no longer need the sdt_types.h file and system-testsuite is compiled as expected.

BZ#718151

The unprivileged probing of user-space applications was not documented properly. This update adds information to the manual pages on unprivileged probing of user-space applications.

BZ#691763

On some architectures, SystemTap could not find certain functions to probe or variables to fetch in highly optimized code. As a consequence, the cxxclass.exp test script failed on PowerPC. This update adds the "-DSTAP_SDT_ARG_CONSTRAINT=nr" option to the cxxclass.exp test script. With this option the arguments are accessible to SystemTap and the test works as expected on PowerPC.

BZ#692445

The stap_run.exp test script incorrectly matched the end of the file and the tests using the script were reported as failed on IBM System z although the tests succeeded. With this update, the end-of-line matching has been fixed and the tests on IBM System z pass as expected.

BZ#723536

The stap command with the "--remote" parameter failed to properly copy the systemtap_session object on Intel x86, PowerPC and IBM System z architectures. Consequently, instrumentation failed to be built and the utility terminated with a segmentation fault. Now, the underlying code copies the systemtap_session object properly and the stap command builds instrumentation as expected.

BZ#723541

The stap command with the "--remote" parameter did not use the proper canonical names on Intel x86, PowerPC and IBM System z architectures. Consequently, instrumentation failed to built. With this update, the underlying session code has been modified to properly copy kernel/arch information and the stap command builds instrumentation correctly in such scenarios.

BZ#738242

On startup, SystemTap needs to allocate memory to individual CPUs for the data transport layer. Previously, SystemTap used the number of all potential CPUs instead of online (schedulable) CPUs to estimate the required memory. Consequently, SystemTap could incorrectly indicate that there was not enough memory available on startup and exit. With this update, the underlying code has been modified and SystemTap now uses the number of online CPUs to estimate the memory needed for data transport layer.

BZ#685064

When probing a user-space module, SystemTap needs the uprobe.ko kernel module. If the module does not exist, it is built. Previously, this could lead to a race condition if multiple scripts probing user-space applications attempted to built the missing uprobes.ko kernel module. The parallel builds of uprobes.ko could interfere with each other and cause the scripts to fail. With this update, the stap command caches the resulting uprobe.ko kernel module to avoid interfering with SystemTap instrumentation instances. Multiple SystemTap scripts probing user-space applications now no longer interfere with each other regardless whether a uprobe.ko kernel module exists.

BZ#684227

The futexes.stp example script in the SystemTap Beginners Guide did not mask out the FUTEX_PRIVATE_FLAG and FUTEX_CLOCK_REALTIME flags in newer versions of the Linux Kernel. Due to this issue, the script could not return any results. The script has been modified and returns the correct results.

BZ#671235

The cmdline_string() function concatenates command line arguments. However, if an empty argument ("") was used, the function did not print any arguments following the NULL argument. The handling of an empty argument was added to the definition of the cmdline_string() function and the

function now prints all arguments from the command line including the arguments following the empty argument.

BZ#607161

There were differences between the tracepoints (kernel.trace(mm_*")) in Red Hat Enterprise Linux and upstream kernels. Due to the differences, the building and running of the mmanonpage and mmfilepage tests failed. This update adds checks which verify the tracepoints' location before running the tests and testsuite only uses the tracepoints on kernels that actually have the tracepoints.

BZ#639344

The syscall wrapper functions used on IBM System z converted arguments from pointers to long integers. The usymbols test assumed the arguments were pointers and the test failed. This update modifies the usymbols test in the SystemTap testsuite package and the utility handles the arguments properly.

BZ#730884

The kernel header files could contain mutually conflicting definitions for the tracepoints of the perf tool. However, SystemTap does not detect kernel headers with conflicting definitions. As the SystemTap translator built the module in one compile unit, the translator tool did not detect the tracepoints. The SystemTap translator now builds instrumention so that the kernel header files with the tracepoints are compiled in seperate units and the tracepoints for jbd and ext3 subsystems are now visible to SystemTap.

BZ#733181

The sdt.exp script ran some tests with -DEXPERIMENTAL_KPROBE_SDT, an obsolete mechanism. On some architectures the tests failed. The sdt.exp script now marks the problematic -DEXPERIMENTAL_KPROBE_SDT that fail as XFAIL. Also, the result of the tests using -DEXPERIMENTAL_KPROBE_SDT that fail are no longer included in the FAIL results.

BZ#733182

The sdt.exp script ran some tests with STAP_SDT_V2, an obsolete mechanism. On some architectures the tests failed because of ambiguities between numeric constants and register numbers. The sdt.exp script now marks the problematic STAP_SDT_V2 that fail as XFAIL. The result of the tests using STAP_SDT_V2 that fail are no longer included in the FAIL results.

BZ#730167

Probing a user-space application requires the uprobes kernel module. Previously, the "--remote" option used the path to the uprobes kernel module on the client instead of the proper path on a remote machine. If a uprobes module was not yet loaded on the remote machine, the instrumentation did not start and the following error message was printed:

```
ERROR: Unable to canonicalize path [...]: No such file or directory
```

SystemTap now loads the correct uprobe module and user-space application probing works as expected with the "--remote" option even if the uprobe kernel module is not currently loaded on remote machine.

BZ#731288

The sdt_misc.exp test did not take into account that some code in sdt_types.c was compiled conditionally, which caused that the number of probe points available could change. As a consequence, the sdt_misc.exp test failed on 32-bit and 64-bit AMD architectures because the

number of probe points available did not match the expected value. With this update, the sdt_misc.exp test now takes into account the conditionally compiled code in sdt_types.c when deciding the number of probe points and the test passes as expected.

Enhancements

BZ#600400

In the verbose mode, the stap-client utility now shows progress information of the communication with the server.

Users of systemtap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.317. T1LIB

4.317.1. RHSA-2012:0062 — Moderate: t1lib security update

Updated t1lib packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The t1lib library allows you to rasterize bitmaps from PostScript Type 1 fonts.

Security Fixes

CVE-2010-2642, CVE-2011-0433

Two heap-based buffer overflow flaws were found in the way t1lib processed Adobe Font Metrics (AFM) files. If a specially-crafted font file was opened by an application linked against t1lib, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-0764

An invalid pointer dereference flaw was found in t1lib. A specially-crafted font file could, when opened, cause an application linked against t1lib to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-1553

A use-after-free flaw was found in t1lib. A specially-crafted font file could, when opened, cause an application linked against t1lib to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-1554

An off-by-one flaw was found in t1lib. A specially-crafted font file could, when opened, cause an application linked against t1lib to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-1552

An out-of-bounds memory read flaw was found in t1lib. A specially-crafted font file could, when opened, cause an application linked against t1lib to crash.

Red Hat would like to thank the Evince development team for reporting CVE-2010-2642. Upstream acknowledges Jon Larimer of IBM X-Force as the original reporter of CVE-2010-2642.

All users of t1lib are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All applications linked against t1lib must be restarted for this update to take effect.

4.318. TCP_WRAPPERS

4.318.1. RHEA-2011:1676 — tcp_wrappers enhancement update

Enhanced tcp_wrappers packages are now available for Red Hat Enterprise Linux 6.

The tcp_wrappers packages provide small daemon programs which can monitor and filter incoming requests for systat, finger, FTP, telnet, rlogin, rsh, exec, tftp, talk and other network services. These packages also contain the libwrap library, which adds the same filtering capabilities to programs linked against it, such as to sshd among others.

Enhancement

BZ#727287

Previously, the tcp_wrappers packages were compiled without the RELRO (read-only relocations) flag. Programs provided by this package and also programs built against the tcp_wrappers libraries were thus vulnerable to various attacks based on overwriting the ELF section of a program. To increase the security of tcp_wrappers programs and libraries, the tcp_wrappers spec file has been modified to use the "-Wl,-z,relro" flags when compiling the packages. As a result, the tcp_wrappers packages are now provided with partial RELRO protection.

Users of tcp_wrappers are advised to upgrade to these updated packages, which add this enhancement.

4.319. TCSH

4.319.1. RHBA-2011:1686 — tcsh bug fix update

An updated tcsh package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

Tcsh is an enhanced and compatible version of the C shell (csh). It is a command language interpreter, which can be used as an interactive login shell, as well as a shell script command processor.

Bug Fixes

BZ#700309

Under certain circumstances when using the cwd symbolic link, a null pointer may have been incorrectly dereferenced, causing the tcsh shell to terminate unexpectedly. With this update, the pointer is now checked properly and tcsh no longer crashes.

BZ#658190

This package fixes the return value of the "status" (or "$?") variable in the case of pipelines and backquoted commands. The "anyerror" variable, which selects the behavior, has been added to retain backward compatibility.

BZ#690356

If the tcsh shell redirected standard output to a child process using a pipe and this child process terminated, the shell tried to print a message to the already-closed pipe as a high-priority event that could never been finished. As a consequence, tcsh entered an infinite loop and consumed up to 100% of the CPU. To fix this issue, this error event is now removed from the event queue before the shell tries to write it to the broken pipe. As result, the parent process terminates ordinarily.

BZ#684063

Prior to this update, the blkend() function was called redundantly in the tsch code. These calls had no effect on tcsh functionality and thus they have been removed. Tcsh functionality remains unchanged and the code is now more effective.

BZ#672592

The tcsh shell allowed variables to named in incorrect formats, such as by allowing a variable name to begin with a digit. This issue has been fixed: variable names are now verified according to Unix variable-naming conventions.

All users of tcsh are advised to upgrade to this updated package, which resolves these issues.

4.319.2. RHBA-2012:0687 — tcsh bug fix update

Updated tcsh packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The tcsh packages contain an enhanced and compatible version of the C shell (csh), which is a command language interpreter, and can be used as an interactive login shell, as well as a shell script command processor.

Bug Fixes

BZ#791232

When using multiple shells simultaneously, the command history is saved from all shells in one ".history" file. Previously, when running multiple csh scripts at the same time, lines in the ".history" file could be reordered with different timestamps or some of the entries could disappear, rendering the ".history" file corrupted. As a consequence, start-up scripts could be slowed down. This update implements file locking mechanism that uses shared readers and an exclusive writer to prevent the ".history" file from being corrupted.

BZ#798652

Previously, the "anyerror" variable could be selected to set the tcsh exit value behavior. However, "anyerror" is a shell variable and therefore was not propagated to subshells, and could not globally affect csh scripts. This update modifies the tcsh exit value behavior to the default behavior of csh: the new "tcsh_posix_status" variable is now available instead of "anyerror" to allow behavior similar to the POSIX standard.

All users of tcsh are advised to upgrade to these updated packages, which fix these bugs.

4.320. TELNET

4.320.1. RHBA-2011:0963 — telnet bug fix update

Updated telnet packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Telnet is a popular protocol for logging in to remote systems over the Internet. The telnet-server package includes a telnet service that supports remote logins into the host machine. The telnet service is disabled by default.

Bug Fix

BZ#678324

Prior to this update, the in.telnetd service used the sockaddr structure to store IPv6 addresses. This structure was too small in its size, and as a result, subsequent logins wrote incorrect records about the last login source. With this update, in.telnetd now uses the sockaddr_storage structure, which is large enough in its size to be able to store IPv6 addresses.

All users of telnet are advised to upgrade to these updated packages, which fix this bug.

4.321. TEXLIVE

4.321.1. RHSA-2012:0137 — Moderate: texlive security update

Updated texlive packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

TeX Live is an implementation of TeX. TeX takes a text file and a set of formatting commands as input, and creates a typesetter-independent DeVice Independent (DVI) file as output. The texlive packages provide a number of utilities, including dvips.

Security Fixes

CVE-2010-2642, CVE-2011-0433

TeX Live embeds a copy of t1lib. The t1lib library allows you to rasterize bitmaps from PostScript Type 1 fonts. The following issues affect t1lib code:

Two heap-based buffer overflow flaws were found in the way t1lib processed Adobe Font Metrics (AFM) files. If a specially-crafted font file was opened by a TeX Live utility, it could cause the utility to crash or, potentially, execute arbitrary code with the privileges of the user running the utility.

CVE-2011-0764

An invalid pointer dereference flaw was found in t1lib. A specially-crafted font file could, when opened, cause a TeX Live utility to crash or, potentially, execute arbitrary code with the privileges of the user running the utility.

CVE-2011-1553

A use-after-free flaw was found in t1lib. A specially-crafted font file could, when opened, cause a TeX Live utility to crash or, potentially, execute arbitrary code with the privileges of the user running the utility.

CVE-2011-1554

An off-by-one flaw was found in t1lib. A specially-crafted font file could, when opened, cause a TeX Live utility to crash or, potentially, execute arbitrary code with the privileges of the user running the utility.

CVE-2011-1552

An out-of-bounds memory read flaw was found in t1lib. A specially-crafted font file could, when opened, cause a TeX Live utility to crash.

Red Hat would like to thank the Evince development team for reporting CVE-2010-2642. Upstream acknowledges Jon Larimer of IBM X-Force as the original reporter of CVE-2010-2642.

All users of texlive are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.322. TEXLIVE-TEXMF

4.322.1. RHBA-2011:1677 — texlive-texmf bug fix update

Updated texlive-texmf packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The texlive-texmf packages contain a texmf distribution based upon TeXLive. TeXLive is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a printable file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX.

Bug Fix

BZ#711344

Prior to this update, LaTeX did not build documents if the source file was more than five years old. An error message appeared and requested manual confirmation which stopped the build process. With this update, the error message has been changed to a message stating that the source file is more than five years old. Now, the build process completes successfully.

All users of texlive-texmf are advised to upgrade to these updated packages, which fix this bug.

4.323. TFTP

4.323.1. RHBA-2012:1436 — ftp bug fix update

Updated ftp packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The ftp packages provide the standard UNIX command line File Transfer Protocol (FTP) client. FTP is a widely used protocol for transferring files over the Internet, and for archiving files.

Bug Fixes

BZ#871059

Previously, the command line width in the ftp client was limited to 200 characters. With this update, the maximum possible length of the FTP command line is extended to 4296 characters.

BZ#871071

Prior to this update, "append", "put", and "send" commands were causing system memory to leak. The memory holding the ftp command was not freed appropriately. With this update, the underlying source code has been improved to correctly free the system resources and the memory leaks are no longer present.

BZ#871546

Previously, if a macro longer than 200 characters was defined and then used after a connection, the ftp client crashed due to a buffer overflow. With this update, the underlying source code was updated and the buffer that holds memory for the macro name was extended. It now matches the length of the command line limit mentioned above. As a result, the ftp client no longer crashes when a macro with a long name is executed.

All users of ftp are advised to upgrade to these updated packages, which fix these bugs.

4.323.2. RHBA-2011:1133 — tftp bug fix update

Updated tftp packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The Trivial File Transfer Protocol (TFTP) is normally used only for booting diskless workstations. The tftp package provides the user interface for TFTP, which allows users to transfer files to and from a remote machine. The tftp-server package provides the server for TFTP which allows users to transfer files to and from a remote machine.

Bug Fixes

BZ#655830

When the small files were transferred and the "-v" option was enabled, the tftp client printed incorrect statistics about the transfer. This update fixes printing of the transfer statistics.

BZ#714240

The tftpd daemon did not correctly handle the utimeout option value. If a client specified a utimeout value within the permitted range, it caused the tftpd process to crash. This crash only affected the current tftp request.

All users of tftp and tftp-server should upgrade to these updated packages, which fix these bugs.

4.324. THUNDERBIRD

4.324.1. RHSA-2012:0080 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple security issues is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-3659

A use-after-free flaw was found in the way Thunderbird removed nsDOMAttribute child nodes. In certain circumstances, due to the premature notification of AttributeChildRemoved, a malicious script could possibly use this flaw to cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0442

Several flaws were found in the processing of malformed content. An HTML mail message containing malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0449

A flaw was found in the way Thunderbird parsed certain Scalable Vector Graphics (SVG) image files that contained eXtensible Style Sheet Language Transformations (XSLT). An HTML mail message containing a malicious SVG image file could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2011-3670

The same-origin policy in Thunderbird treated http://example.com and http://[example.com] as interchangeable. A malicious script could possibly use this flaw to gain access to sensitive information (such as a client's IP and user e-mail address, or httpOnly cookies) that may be included in HTTP proxy error replies, generated in response to invalid URLs using square brackets.

Note: The CVE-2011-3659 and CVE-2011-3670 issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. It could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

For technical details regarding these flaws, refer to the Mozilla security advisories for Thunderbird 3.1.18.:

http://www.mozilla.org/security/known-vulnerabilities/thunderbird31.html#thunderbird3.1.18

All Thunderbird users should upgrade to these updated packages, which contain Thunderbird version 3.1.18, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.324.2. RHSA-2012:0140 — Critical: thunderbird security update

An updated thunderbird package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fix

CVE-2011-3026

A heap-based buffer overflow flaw was found in the way Thunderbird handled PNG (Portable Network Graphics) images. An HTML mail message or remote content containing a specially-crafted

PNG image could cause Thunderbird to crash or, possibly, execute arbitrary code with the privileges of the user running Thunderbird.

All Thunderbird users should upgrade to this updated package, which corrects this issue. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.324.3. RHSA-2012:0388 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2012-0461, CVE-2012-0462, CVE-2012-0464

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0456, CVE-2012-0457

Two flaws were found in the way Thunderbird parsed certain Scalable Vector Graphics (SVG) image files. An HTML mail message containing a malicious SVG image file could cause an information leak, or cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0455

A flaw could allow malicious content to bypass intended restrictions, possibly leading to a cross-site scripting (XSS) attack if a user were tricked into dropping a "javascript:" link onto a frame.

CVE-2012-0458

It was found that the home page could be set to a "javascript:" link. If a user were tricked into setting such a home page by dragging a link to the home button, it could cause Firefox to repeatedly crash, eventually leading to arbitrary code execution with the privileges of the user running Firefox. A similar flaw was found and fixed in Thunderbird.

CVE-2012-0459

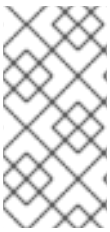
A flaw was found in the way Thunderbird parsed certain, remote content containing "cssText". Malicious, remote content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0460

It was found that by using the DOM fullscreen API, untrusted content could bypass the mozRequestFullscreen security protections. Malicious content could exploit this API flaw to cause user interface spoofing.

CVE-2012-0451

A flaw was found in the way Thunderbird handled content with multiple Content Security Policy (CSP) headers. This could lead to a cross-site scripting attack if used in conjunction with a website that has a header injection flaw.



NOTE

All issues except CVE-2012-0456 and CVE-2012-0457 cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. It could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 10.0.3 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.324.4. RHSA-2012:0516 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-3062

A flaw was found in Sanitiser for OpenType (OTS), used by Thunderbird to help prevent potential exploits in malformed OpenType fonts. Malicious content could cause Thunderbird to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0467, **CVE-2012-0468**, **CVE-2012-0469**

Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0470

Content containing a malicious Scalable Vector Graphics (SVG) image file could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0472

A flaw was found in the way Thunderbird used its embedded Cairo library to render certain fonts. Malicious content could cause Thunderbird to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0478

A flaw was found in the way Thunderbird rendered certain images using WebGL. Malicious content could cause Thunderbird to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0471

A cross-site scripting (XSS) flaw was found in the way Thunderbird handled certain multibyte character sets. Malicious content could cause Thunderbird to run JavaScript code with the permissions of different content.

CVE-2012-0473

A flaw was found in the way Thunderbird rendered certain graphics using WebGL. Malicious content could cause Thunderbird to crash.

CVE-2012-0474

A flaw in the built-in feed reader in Thunderbird allowed the Website field to display the address of different content than the content the user was visiting. An attacker could use this flaw to conceal a malicious URL, possibly tricking a user into believing they are viewing a trusted site, or allowing scripts to be loaded from the attacker's site, possibly leading to cross-site scripting (XSS) attacks.

CVE-2012-0477

A flaw was found in the way Thunderbird decoded the ISO-2022-KR and ISO-2022-CN character sets. Malicious content could cause Thunderbird to run JavaScript code with the permissions of different content.

CVE-2012-0479

A flaw was found in the way the built-in feed reader in Thunderbird handled RSS and Atom feeds. Invalid RSS or Atom content loaded over HTTPS caused Thunderbird to display the address of said content, but not the content. The previous content continued to be displayed. An attacker could use this flaw to perform phishing attacks, or trick users into thinking they are visiting the site reported by the Website field, when the page is actually content controlled by an attacker.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Mateusz Jurczyk of the Google Security Team as the original reporter of CVE-2011-3062; Aki Helin from OUSPG as the original reporter of CVE-2012-0469; Atte Kettunen from OUSPG as the original reporter of CVE-2012-0470; wushi of team509 via iDefense as the original reporter of CVE-2012-0472; Ms2ger as the original reporter of CVE-2012-0478; Anne van Kesteren of Opera Software as the original reporter of CVE-2012-0471; Matias Juntunen as the original reporter of CVE-2012-0473; Jordi Chancel and Eddy Bordi, and Chris McGowen as the original reporters of CVE-2012-0474; Masato Kinugawa as the original reporter of CVE-2012-0477; and Jeroen van der Gun as the original reporter of CVE-2012-0479.

NOTE

All issues except CVE-2012-0470, CVE-2012-0472, and CVE-2011-3062 cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. It could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.324.5. RHSA-2012:0715 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6.

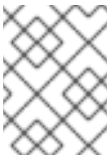
The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-3101, **CVE-2012-1937**, **CVE-2012-1938**, **CVE-2012-1939**, **CVE-2012-1940**, **CVE-2012-1941**, **CVE-2012-1946**, **CVE-2012-1947**

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.



NOTE

Note: CVE-2011-3101 only affected users of certain NVIDIA display drivers with graphics cards that have hardware acceleration enabled.

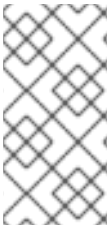
CVE-2012-1944

It was found that the Content Security Policy (CSP) implementation in Thunderbird no longer blocked Thunderbird inline event handlers. Malicious content could possibly bypass intended restrictions if that content relied on CSP to protect against flaws such as cross-site scripting (XSS).

CVE-2012-1945

If a web server hosted content that is stored on a Microsoft Windows share, or a Samba share, loading such content with Thunderbird could result in Windows shortcut files (.lnk) in the same share also being loaded. An attacker could use this flaw to view the contents of local files and directories on the victim's system. This issue also affected users opening content from Microsoft Windows shares, or Samba shares, that are mounted on their systems.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Ken Russell of Google as the original reporter of CVE-2011-3101; Igor Bukanov, Olli Pettay, Boris Zbarsky, and Jesse Ruderman as the original reporters of CVE-2012-1937; Jesse Ruderman, Igor Bukanov, Bill McCloskey, Christian Holler, Andrew McCreight, and Brian Bondy as the original reporters of CVE-2012-1938; Christian Holler as the original reporter of CVE-2012-1939; security researcher Abhishek Arya of Google as the original reporter of CVE-2012-1940, CVE-2012-1941, and CVE-2012-1947; security researcher Arthur Gerkis as the original reporter of CVE-2012-1946; security researcher Adam Barth as the original reporter of CVE-2012-1944; and security researcher Paul Stone as the original reporter of CVE-2012-1945.



NOTE

None of the issues in this advisory can be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 10.0.5 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.325. TMPWATCH

4.325.1. RHBA-2011:1199 — tmpwatch bug fix update

An updated tmpwatch package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The tmpwatch utility recursively searches through specified directories and removes files which have not been accessed in a specified period of time. Tmpwatch is normally used to clean up directories which are used for temporarily holding files (for example, /tmp).

Bug Fix

BZ#722856

When searching for files or directories to remove, tmpwatch was reporting all failures to access these files or directories. This included expected access failures due to the restrictive default configuration of FUSE mount points. With this update, tmpwatch now silently ignores all EACCES errors, and the expected access failures regarding FUSE mount points are no longer reported.

All users are advised to upgrade to this updated tmpwatch package, which fixes this bug.

4.326. TOG-PEGASUS

4.326.1. RHBA-2011:1563 — tog-pegasus bug fix and enhancement update

Updated tog-pegasus packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

OpenPegasus WBEM Services for Linux enable management solutions that deliver increased control of enterprise resources. Web-Based Enterprise Management (WBEM) is a platform and resource independent Distributed Management Task Force (DMTF) standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.

These updated packages upgrade tog-pegasus to the more recent upstream version 2.11.0, which provides a number of bug fixes and enhancements over the previous packaged version. (BZ#633577)

Bug Fixes

BZ#607722

Previously, tog-pegasus did not comply with Red Hat multilib policy. This update moves the runtime libraries into the new tog-pegasus-libs subpackage. Now, tog-pegasus is in complience with the multilib policy.

BZ#693389

Previously, binaries in tog-pegasus were stripped of their debuginfo files during the build process. As a consequence, the debuginfo files were missing and could prevent correct debugging of crashes. This update modifies the code and binaries are no longer stripped of the debug information.

Enhancements

BZ#694513

This update adds the external SLP and Privilege Separation options to provide support for IBM Systems Director.

BZ#712525

This update adds OpenSLP support to tog-pegasus.

All users of tog-pegasus are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.327. TOMCAT6

4.327.1. RHSA-2012:0475 — Moderate: tomcat6 security update

Updated tomcat6 packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Security Fixes

CVE-2011-4858

It was found that the Java hashCode() method implementation was susceptible to predictable hash collisions. A remote attacker could use this flaw to cause Tomcat to use an excessive amount of CPU time by sending an HTTP request with a large number of parameters whose names map to the same hash value. This update introduces a limit on the number of parameters processed per request to mitigate this issue. The default limit is 512 for parameters and 128 for headers. These defaults can be changed by setting the org.apache.tomcat.util.http.Parameters.MAX_COUNT and org.apache.tomcat.util.http.MimeHeaders.MAX_COUNT system properties.

CVE-2012-0022

It was found that Tomcat did not handle large numbers of parameters and large parameter values efficiently. A remote attacker could make Tomcat use an excessive amount of CPU time by sending an HTTP request containing a large number of parameters or large parameter values. This update introduces limits on the number of parameters and headers processed per request to address this issue. Refer to the CVE-2011-4858 description for information about the org.apache.tomcat.util.http.Parameters.MAX_COUNT and org.apache.tomcat.util.http.MimeHeaders.MAX_COUNT system properties.

Red Hat would like to thank oCERT for reporting CVE-2011-4858. oCERT acknowledges Julian Wälde and Alexander Klink as the original reporters of CVE-2011-4858.

Users of Tomcat should upgrade to these updated packages, which correct these issues. Tomcat must be restarted for this update to take effect.

4.328. TOMCATJSS

4.328.1. RHBA-2011:1674 — tomcatjss bug fix update

An updated tomcatjss package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The tomcatjss package provides a Java Secure Socket Extension (JSSE) implementation using Java Security Services (JSS) for Tomcat 6.

Bug Fix

BZ#705107

If the server "admin" port was configured to accept a specific client authentication certificate, such as SSL (Secure Sockets Layer) certificate, other alternative authentication types failed even if the port was configured to accept them. The underlying code has been modified and the alternative authentication types are successful if called upon.

All tomcatjss users are advised to upgrade to this updated package, which fixes this bug.

4.329. TSCLIENT

4.329.1. RHBA-2011:1662 — tsclient bug fix update

An updated tsclient package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The tsclient utility is a GTK2 front end that makes it easy to use the Remote Desktop Protocol client (rdesktop) and vncviewer utilities.

Bug Fix

BZ#667684

Previously, the tsclient utility did not provide a "Client Hostname" option. Users experienced the "No valid license available" error message from the terminal server after many successful connections. To solve this problem an option to enter client hostname information, "-n", has been added. Now, the user can enter client hostname information and it will be passed to the rdesktop client.

All users of tsclient are advised to upgrade to this updated package which fixes this bug.

4.330. TUNED

4.330.1. RHBA-2011:1176 — tuned bug fix update

Updated tuned packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The "tuned" packages contain a daemon that tunes system settings dynamically. It does so by monitoring the usage of several system components periodically.

Bug Fixes

BZ#695480

Previously, remote "tuned" service starts could have led to a service unresponsiveness under certain circumstances. With this update, the handling of stdin, stdout, or stderr during the service creation has been fixed to resolve this problem.

BZ#707079

Previously, using NIC bonding could have led to an unexpected termination of "tuned". With this update, the network device type determination has been fixed by handling more error conditions so that the aforementioned bug no longer occurs.

All users of "tuned" are advised to upgrade to these updated packages, which fix these bugs.

4.331. UDEV

4.331.1. RHBA-2011:1649 — udev bug fix and enhancement update

Updated udev packages that fix various bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

The udev packages implement a dynamic device-directory, providing only the devices present on the system. This dynamic directory runs in user space, dynamically creates and removes devices, provides consistent naming, and a user-space API. The udev package replaces the devfs package and provides better hot plug functionality.

Bug Fixes

BZ#632646

Previously, a udev rule used the modem-modeswitch callout on the Vodafone K3565-Z 3G modem. As a consequence, a medium in a virtual CD-ROM drive could not be ejected to activate the modem functionality. Now, the modem-modeswitch callout is no longer used for this device and a medium is automatically ejected instead, thus fixing this bug.

BZ#698540

The path_id utility did not create symbolic links for SAS (Serial Attached SCSI) devices without enclosures. Consequently, udev did not create a symbolic link in the /dev/disk/by-path/ directory and the device could not be accessed by this path. This bug has been fixed, udev now follows the naming scheme of its upstream version 171, and symbolic links for SAS devices are now created in the following format: sas-[sas_address]-[lun]". In this format, [sas_address] stands for the contents of the sas_address file of the device, located in the /sys subdirectory, and [lun] represents the logical unit number of the device.

BZ#714951

The path_id utility did not create symbolic links for iSCSI (Internet SCSI) devices. Consequently, udev did not create a symbolic link in the /dev/disk/by-path/ directory and the device could not be accessed by this path. This bug has been fixed, udev now follows the naming scheme of its upstream version 171, and symbolic links for iSCSI devices are now created in the following format: "ip-[address]:[port]-iscsi-[target]-[lun]". In this format, [lun] represents the logical unit number of the device.

BZ#701265

When udev renamed a network interface and encountered a naming conflict, it renamed the interface to "[initial name]-[desired name]". Sometimes, this name was not unique and the naming conflict persisted. This bug has been fixed, udev now uses the unique interface index for renaming, and temporary names for interfaces are now of the following format: "rename[ifindex]".

BZ#727500

Prior to this update, the libgudev1 package had no explicit package version requirement on the libudev library. As a consequence, it was possible to update libudev without updating libgudev1, which could lead to inconsistencies, if the ABI (application binary interface) changed in libudev. With

this update, the libgudev1 spec file has been updated, and the package now requires libudev explicitly, thus fixing this bug.

BZ#726566

Previously, the result buffer to store the output of programs started with the IMPORT directive was too short in some cases. Consequently, the "ERR udevd-work: ressize 4096 too short" error messages were returned, and the system sometimes became non-operational. Now, the result buffer has been increased to 16kB, thus fixing this bug.

BZ#696651

Previously, when traversing the list of devices internal to udev, the libvirtd daemon terminated unexpectedly in the udev_enumerate_get_list_entry() function. This bug has been fixed and libvirtd no longer crashes in the described scenario.

BZ#731400

Previously, for Xen block devices, udev did not provide information acquired by the blkid utility, such as the filesystem label or UUID. Consequently, no symbolic links in the /dev/disk/{by-uuid,by-label,by-id} directories were created. With this update, these symbolic links are created for Xen block devices as expected, thus fixing this bug.

Enhancement

BZ#711254

The default I/O scheduler (CFQ) parameters for all disk types, except SATA disks, have been changed as follows:

```
slice_idle=0
quantum=32
```

All users of udev are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.332. UDISKS

4.332.1. RHBA-2011:1764 — udisks bug fix update

An updated udisks package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The udisks daemon provides interfaces to obtain information and perform operations on storage devices.

Bug Fix

BZ#738479

Prior to this update, the redundant udev watch rule interfered with the Logical Volume Manager (LVM) which could cause problems under certain workloads. This update removes this udev rule and udisks no longer interferes with LVM.

All users of udisks are advised to upgrade to this updated package, which fixes this bug.

4.333. UNICAP

4.333.1. RHBA-2011:1202 — unicap bug fix update

An updated unicap package that fixes multiple bugs is now available for Red Hat Enterprise Linux 6.

The unicap package provides a uniform interface to video capture devices. It allows applications to use any supported video capture device via a single application programming interface (API). The included ucil library provides functions to render text and graphic overlays onto video images.

Bug Fixes

BZ#612693

Prior to this update, the unicap package did not provide the libucil, libunicap and libunicap-gtk virtual packages. As a result, it was not possible to install packages that depended on the libucil, libunicap and libunicap-gtk packages. This update fixes the declaration "--provides" so that the unicap package now provides the virtual packages.

BZ#635644

Prior to this update, the unicap utility did not check for the return value of the Advanced Linux Sound Architecture (ALSA) initialization. As a result, unicap terminated unexpectedly if the initialization of ALSA failed. This update adds the missing checks for the return value to handle the ALSA initialization failure gracefully.

BZ#635645

Prior to this update, the unicap utility did not check for the return value of the Theora encoder initialization. As a result, unicap terminated unexpectedly if the initialization of the Theora encoder failed. This update adds the missing checks for the return value to handle the Theora encoder initialization failure gracefully.

BZ#658059

Prior to this update, unicap-devel packages for both 32-bit and 64-bit architectures on a single system could not be installed because of conflicts between the packages. This update uses the documentation from the unicap source code archive instead of the documentation generated at build time. Now, unicap-devel packages can be installed as expected.

BZ#728473

Prior to this update, the unicap package was missing a dependency on libv4l2.so.0, although some libraries shipped with unicap were using libv4l2.so.0. This update adds the missing dependency.

All users of unicap are advised to upgrade to this updated package, which fixes these bugs.

4.334. USBUTILS

4.334.1. RHBA-2011:1646 — usbutils bug fix and enhancement update

An updated usbutils package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The usbutils package contains utilities for inspecting devices connected to a USB bus.

The usbutils package has been upgraded to upstream version 003, which adds support for USB3 devices. Note: warning messages about short transfer on control endpoint and stalled endpoint can under circumstances be logged after the upgrade. This is the standard behavior of the xHCI driver and these messages can be safely ignored. This update also provides a number of bug fixes and enhancements over the previous version. (BZ#725973, BZ#725096)

Bug Fixes

BZ#725982

Previously, when running the "lsusb -t" command in a KVM guest, the lsusb utility terminated with a segmentation fault. The utility has been modified and now lists USB devices correctly.

BZ#730671

The FILES item in the lsusb(8) manual page displayed an incorrect path to the usb.ids file. This path has been changed to the correct /usr/share/hwdata/usb.ids path.

All users of usbutils are advised to upgrade to this updated usbutils package, which fixes these bugs and adds these enhancements.

4.335. UTIL-LINUX-NG

4.335.1. RHSA-2011:1691 — Low: util-linux-ng security, bug fix, and enhancement update

Updated util-linux-ng packages that fix multiple security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The util-linux-ng packages contain a large variety of low-level system utilities that are necessary for a Linux operating system to function.

Security Fixes

CVE-2011-1675, CVE-2011-1677

Multiple flaws were found in the way the mount and umount commands performed mtab (mounted file systems table) file updates. A local, unprivileged user allowed to mount or unmount file systems could use these flaws to corrupt the mtab file and create a stale lock file, preventing other users from mounting and unmounting file systems.

Bug Fixes

BZ#675999

Due to a hard coded limit of 128 devices, an attempt to run the "blkid -c" command on more than 128 devices caused blkid to terminate unexpectedly. This update increases the maximum number of devices to 8192 so that blkid no longer crashes in this scenario.

BZ#679741

Previously, the "swapon -a" command did not detect device-mapper devices that were already in use. This update corrects the swapon utility to detect such devices as expected.

BZ#684203

Prior to this update, the presence of an invalid line in the /etc/fstab file could cause the umount utility to terminate unexpectedly with a segmentation fault. This update applies a patch that corrects this error so that umount now correctly reports invalid lines and no longer crashes.

BZ#696959

Previously, an attempt to use the wipefs utility on a partitioned device caused the utility to terminate unexpectedly with an error. This update adapts wipefs to only display a warning message in this situation.

BZ#712158

When providing information on interprocess communication (IPC) facilities, the ipcs utility could previously display a process owner as a negative number if the user's UID was too large. This update adapts the underlying source code to make sure the UID values are now displayed correctly.

BZ#712808

In the installation scriptlets, the uuidd package uses the chkconfig utility to enable and disable the uuidd service. Previously, this package did not depend on the chkconfig package, which could lead to errors during installation if chkconfig was not installed. This update adds chkconfig to the list of dependencies so that such errors no longer occur.

BZ#716995

The previous version of the /etc/udev/rules.d/60-raw.rules file contained a statement that both this file and raw devices are deprecated. This is no longer true and the Red Hat Enterprise Linux kernel supports this functionality. With this update, the aforementioned file no longer contains this incorrect statement.

BZ#723352

Previously, an attempt to use the cfdisk utility to read the default Red Hat Enterprise Linux 6 partition layout failed with an error. This update corrects this error and the cfdisk utility can now read the default partition layout as expected.

BZ#679831

The previous version of the tailf(1) manual page incorrectly stated that users can use the "--lines=NUMBER" command line option to limit the number of displayed lines. However, the tailf utility does not allow the use of the equals sign (=) between the option and its argument. This update corrects this error.

BZ#694648

The fstab(5) manual page has been updated to clarify that empty lines in the /etc/fstab configuration file are ignored.

Enhancements

BZ#692119

A new fstrim utility has been added to the package. This utility allows the root user to discard unused blocks on a mounted file system.

BZ#696731

The login utility has been updated to provide support for failed login attempts that are reported by PAM.

BZ#723638

The lsblk utility has been updated to provide additional information about the topology and status of block devices.

BZ#726092

The agetty utility has been updated to pass the hostname to the login utility.

All users of util-linux-ng are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements.

4.336. VALGRIND

4.336.1. RHBA-2011:1651 — valgrind bug fix and enhancement update

Updated valgrind packages that fix several bugs and add an enhancement are available for Red Hat Enterprise Linux 6.

Valgrind is a tool to help users find memory management problems in programs. Valgrind can detect a lot of problems that are otherwise very hard to find or diagnose.

Bug Fixes

BZ#708522

When building the valgrind package with macros to prevent application of any downstream patches, the rebuild process failed. This bug has been fixed and valgrind can now be properly rebuilt in the described scenario.

BZ#713956

Previously, the JIT (Just in Time Compiler) in some versions of the JDK (Java Development Kit) generated useless, but valid, instruction prefixes, which valgrind could not emulate. Consequently, Java applications running under valgrind sometimes terminated unexpectedly. With this update, valgrind has been changed to emulate instructions even with these useless prefixes, the JVM process now exits properly, and valgrind displays memory leak summary information in the described scenario.

BZ#717218

In a Coverity Scan analysis, a redundant check was discovered in one of the backported patches applied to the valgrind package. An upstream patch has been applied to address this issue and the redundant check is no longer performed.

Enhancement

BZ#694598

With this update, the valgrind package has been updated to provide support for 64-bit IBM POWER7 Series hardware.

Users of valgrind are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.337. VIRT-MANAGER

4.337.1. RHBA-2011:1642 — virt-manager bug fix and enhancement update

An updated virt-manager package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

Virtual Machine Manager (virt-manager) is a graphical tool for administering virtual machines for KVM, Xen, and QEMU.

The virt-manager package has been upgraded to upstream version 0.9.0, which provides support for the IEEE 802.1Qbg standard. The virt-manager utility now allows editing of virtualport settings for direct interfaces. (BZ#693875)

Bug Fixes

BZ#703067

If the user pressed the X button on the "Customize configuration before install" dialog box, the box closed and the installation started instead of being canceled. With this update, pressing the new Cancel button in the dialog box removes the custom changes and displays the "New VM" wizard. The X button now correctly performs the cancel action.

BZ#729590

The virt-manager utility offered sound card models in the user interface (UI) that are not supported at the QEMU level. As a consequence, selecting one of these models prevented a guest from starting. Unsupported models are now hidden so that there is no option to generate a broken guest configuration.

BZ#699953

When performing tunneled migration using the virt-manager utility, the migration failed with an error message. With this update, the proper URI is now generated when performing peer-to-peer migration. As a result, tunneled migration now works as expected.

BZ#727766

The virt-manager utility offered to create the SCSI (Small Computer System Interface) and USB devices in the UI. These options are not supported at the QEMU level, therefore selecting one of these models prevented a guest from starting. Unsupported models are now hidden so that there is no option to generate a broken guest configuration.

BZ#732371

Previously, virt-manager did not properly escape reserved characters in domain names when listing them in the main list of virtual machines. If a virtual machine had any reserved XML characters in its name, the name was incorrectly displayed in the list of virtual machines. With this update, virt-manager properly escapes reserved characters in the names of virtual machines, which are correctly displayed as a result.

BZ#588505

When monitoring the disk I/O statistics in virt-manager, the utility used different scales on graphs for various machines. As a consequence, a graph for a virtual machine with low I/O activity displayed

very similar information as a graph for a machine with high I/O activity. The virt-manager utility is now modified to show all visible graphs on the same scale, adjusted dynamically to the highest reported I/O value. Graphs can now be reliably compared across various virtual machines.

BZ#698096

Previously, virt-manager incorrectly compared USB devices of a running guest to the USB devices from its offline configuration file. A hot unplugged USB device did appear again after the guest had been rebooted. Now, comparisons work correctly for online and offline guests and hot unplug removes the USB device for all subsequent starts.

Enhancements

BZ#488141

The virt-manager utility now provides an option to set the iSCSI Qualified Name (IQN) value for an iSCSI pool.

BZ#680060

With this update, virt-manager now uses the Simple Protocol for Independent Computing Environments (SPICE) graphics for new guests by default. This allows for audio streaming and better graphics performance.

BZ#546440

Previously, only local guest virtual machines were allowed to be installed by specifying a URL tree. With this update, virt-manager can now provision also remote guests using a URL tree.

BZ#693872

The virt-manager utility now allows managing Linux Containers (LXC) guests. This includes basic life cycle management (start, stop, pause) and creation of application containers.

Users are advised to upgrade to this updated virt-manager package, which fixes these bugs and adds these enhancements.

4.338. VIRT-TOP

4.338.1. RHBA-2011:1692 — virt-top bug fix and enhancement update

An updated virt-top package that fixes three bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The virt-top utility displays statistics of virtualized domains and uses many of the same keys and command line options as the top utility.

Bug Fixes

BZ#730208

Prior to this update, the terminal was not properly restored if the --csv flag was given. This update modifies the code so that the terminal is now restored in the correct mode.

BZ#665817

The CSV output of virt-top contains only the headers for the first virtual machine. This update adds a processcsv.py script to virt-top so that the CSV output can now be split up into multiple files, each file containing full headers.

BZ#680031

When a libvirt error happens early during virt-top start-up, an obscure error message can be printed. With this update, the manual page contains added instructions for debugging libvirt errors that can occur during program initialization.

Enhancement

BZ#680027

With this update, the domain memory information is now displayed in the CSV output mode.

All virt-top users are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.339. VIRT-V2V

4.339.1. RHSA-2011:1615 — Low: virt-v2v security and bug fix update

An updated virt-v2v package that fixes one security issue and several bugs is now available for Red Hat Enterprise Linux 6.

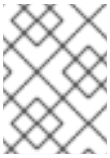
The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

virt-v2v is a tool for converting and importing virtual machines to libvirt-managed KVM (Kernel-based Virtual Machine), or Red Hat Enterprise Virtualization.

Security Fix

CVE-2011-1773

Using virt-v2v to convert a guest that has a password-protected VNC console to a KVM guest removed that password protection from the converted guest: after conversion, a password was not required to access the converted guest's VNC console. Now, converted guests will require the same VNC console password as the original guest. Note that when converting a guest to run on Red Hat Enterprise Virtualization, virt-v2v will display a warning that VNC passwords are not supported.



NOTE

The Red Hat Enterprise Linux 6.2 perl-Sys-Virt update must also be installed to correct CVE-2011-1773.

Bug Fixes

BZ#665883

When converting a guest virtual machine (VM), whose name contained certain characters, virt-v2v would create a converted guest with a corrupted name. Now, virt-v2v will not corrupt guest names.

BZ#671094

There were numerous usability issues when running virt-v2v as a non-root user. This update makes it simpler to run virt-v2v as a non-root user.

BZ#673066

virt-v2v failed to convert a Microsoft Windows guest with Windows Recovery Console installed in a separate partition. Now, virt-v2v will successfully convert a guest with Windows Recovery Console installed in a separate partition by ignoring that partition.

BZ#694364

virt-v2v failed to convert a Red Hat Enterprise Linux guest which did not have the symlink "/boot/grub/menu.lst". With this update, virt-v2v can select a grub configuration file from several places.

BZ#694370

This update removes information about the usage of deprecated command line options in the virt-v2v man page.

BZ#696089

virt-v2v would fail to correctly change the allocation policy, (sparse or preallocated) when converting a guest with QCOW2 image format. The error message "Cannot import VM, The selected disk configuration is not supported" was displayed. With this update, allocation policy changes to a guest with QCOW2 storage will work correctly.

BZ#700759

The options "--network" and "--bridge" can not be used in conjunction when converting a guest, but no error message was displayed. With this update, virt-v2v will now display an error message if the mutually exclusive "--network" and "--bridge" command line options are both specified.

BZ#702007

virt-v2v failed to convert a multi-boot guest, and did not clean up temporary storage and mount points after failure. With this update, virt-v2v will prompt for which operating system to convert from a multi-boot guest, and will correctly clean up if the process fails.

BZ#707261

virt-v2v failed to correctly configure modprobe aliases when converting a VMware ESX guest with VMware Tools installed. With this update, modprobe aliases will be correctly configured.

BZ#727489

When converting a guest with preallocated raw storage using the libvirtxml input method, virt-v2v failed with the erroneous error message "size(X) < usage(Y)". This update removes this erroneous error.

BZ#708961

When converting a Red Hat Enterprise Linux guest, virt-v2v did not check that the Cirrus X driver was available before configuring it. With this update, virt-v2v will attempt to install the Cirrus X driver if it is required.

BZ#732421

VirtIO systems do not support the Windows Recovery Console on 32-bit Windows XP. The virt-v2v man page has been updated to note this. On Windows XP Professional x64 Edition, however, if Windows Recovery Console is re-installed after conversion, it will work as expected.

BZ#677870

Placing comments in the guest fstab file by means of the leading "#" symbol caused an "unknown filesystem" error after conversion of a guest. With this update comments can now be used and error messages will not be displayed.

Users of virt-v2v should upgrade to this updated package, which fixes these issues and upgrades virt-v2v to version 0.8.3.

4.340. VIRT-VIEWER

4.340.1. RHEA-2011:1614 — virt-viewer bug fix and enhancement update

An updated virt-viewer package that fixes several bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

Virtual Machine Viewer (virt-viewer) is a lightweight interface for interacting with the graphical display of a virtualized quest. It uses libvirt and is intended as a replacement for traditional VNC clients.

The virt-viewer package has been upgraded to upstream version 0.4.1, which provides support for The Simple Protocol for Independent Computing Environments (SPICE) multihead setups. (BZ#680213)

Bug Fixes

BZ#680331

Running the virt-viewer utility with the "--verbose" or "-v" option did not display verbose information. With this update, additional data has been provided so that the command outputs detailed information.

BZ#730346

Previously, the virt-viewer utility failed to connect to remote displays when using SSH tunneling with the SSH server on a non-standard port number. An upstream patch has been applied to address this issue and virt-viewer now correctly displays remote quests.

BZ#730901

Previously, running the "virt-viewer --zoom" command with a zoom level specified did not work correctly. This update fixes the initial zoom level on a display, and the primary window zoom level is now propagated to secondary windows. As a result, the zoom option works as expected.

BZ#730911

Using a wildcard address (for example, 0.0.0.0) as a listen address for the graphic server could cause virt-viewer to fail to connect to remote virtual machines. If the user used the "virt-viewer --direct --connect" command with a remote IP address to connect a virtual machine, virt-viewer connected to the graphic server but was not able to connect to the virtual machine. The hostname is now used from the libvirt URI and virt-viewer can open remote virtual machines successfully.

BZ#731132

Due to an invalid implementation of the libvirt events API, the virt-viewer utility occasionally resulted in a deadlock. To avoid deadlock situations, ff callbacks are now invoked from a clean stack instead of being called directly from the remote callback.

BZ#739007

Previously, the window titles for virt-viewer instances did not contain the name of the displayed guest, nor did they contain the number of guest displays (for multihead setups). The source code has been modified so that the titles now contain both the name of the guest and the number of displays.

BZ#740724

Guests are normally configured with their VNC (Virtual Network Computing) server on a TCP socket, but can be also configured to use a UNIX domain socket instead. Prior to this update, virt-viewer was unable to connect to such a guest and terminated unexpectedly with a segmentation fault when attempting to open it. A patch has been applied to address the issue and the virt-viewer utility now opens guests successfully and no longer crashes.

BZ#744370

Due to certain broken key combinations, sending the Ctrl+Alt+F9 and Ctrl+Alt+F10 key combinations incorrectly opened the tty4 and tty5 text consoles in virt-viewer. This update fixes the broken key combinations and the text console no longer opens when sending the aforementioned key combinations.

BZ#744374

Previously, the window title was missing the guestname when waiting for a domain to start. To fix this problem, the initial window title is set to the "--wait" command line argument while waiting for a virtual machine to start. When the machine actually appears, the title is updated to the real name of the machine.

BZ#744377

With the SPICE (Simple Protocol for Independent Computing Environments) graphics, the virt-viewer windows did not display the "Press Ctrl+Alt to release pointer" information. With this update, VirtViewerDisplaySpice is connected to the grab signals in DisplaySpice, which ensures that the release sequence message is now displayed.

Users are advised to upgrade to this updated virt-viewer package, which fixes these bugs and adds this enhancement.

4.341. VIRT-WHAT

4.341.1. RHEA-2011:1556 — virt-what bug fix and enhancement update

An updated virt-what package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The virt-what package provides a command line tool that is used to detect whether the operating system is running inside a virtual machine.

The virt-what package has been upgraded to upstream version 1.11, which provides a number of bug fixes and enhancements over the previous version. (BZ#672211)

Bug Fix

BZ#707524

On the 64-bit x86 architecture, if the user configured a CPU model for the virtual machine, the virt-what utility failed to detect that the guest was running inside a virtual machine. The order of tests has been rearranged, fixing the problem.

Users of virt-what are advised to upgrade to this updated package which fixes these bugs and adds these enhancements.

4.342. VSFTPD

4.342.1. RHBA-2012:0001 — vsftpd bug fix update

An updated vsftpd package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The vsftpd package includes a Very Secure FTP (File Transfer Protocol) daemon.

Bug Fix

BZ#767108

The vsftpd daemon sets a value of the RLIMIT_AS variable during its initialization phase. With Red Hat Enterprise Linux 6.1, the RLIMIT_AS value (100 MB) became insufficient which restricted LDAP users from authentication to the system using vsftpd. With this update, the initial RLIMIT_AS value has been increased to 200 MB, and vsftpd now can be used for LDAP authentication as expected.

All users of vsftpd are advised to upgrade to this updated package, which fixes this bug.

4.343. VTE

4.343.1. RHBA-2011:1204 — vte bug fix update

An updated vte package that fixes one bug is now available for Red Hat Enterprise Linux 6.

VTE is a terminal emulator widget for use with GTK+ 2.0.

Bug Fix

BZ#658774

Previously, setting a cursor color was not working properly in that a terminal (text) cursor was invisible in some applications which used vte. With this update, the bug has been fixed so that the cursor is now rendered properly and is visible as expected.

All vte users are advised to upgrade to this updated package, which fixes this bug.

4.344. WHICH

4.344.1. RHBA-2011:0911 — which bug fix update

An updated which package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The "which" package includes the "which" command that shows the full pathname of a specified program, if the specified program is in your PATH.

Bug Fix

BZ#671289

Prior to this update, the /etc/profile.d/which2.csh file caused an alias for the "which" command to be created. As a result, the "which" command included in the "which" package was used instead of the built-in "which" command as included in the C shell (csh). The problem has been fixed in this update by removing the /etc/profile.d/which2.csh file so that the "which" command included in csh is now used as expected.

All users of "which" should upgrade to this updated package, which fixes this bug.

4.345. WIRESHARK

4.345.1. RHSA-2012:0509 — Moderate: wireshark security update

Updated wireshark packages that fix several security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

Security Fixes

CVE-2011-1590, **CVE-2011-4102**, **CVE-2012-1595**

Several flaws were found in Wireshark. If Wireshark read a malformed packet off a network or opened a malicious dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark.

CVE-2011-1143, **CVE-2011-1957**, **CVE-2011-1958**, **CVE-2011-1959**, **CVE-2011-2174**, **CVE-2011-2175**, **CVE-2011-2597**, **CVE-2011-2698**, **CVE-2012-0041**, **CVE-2012-0042**, **CVE-2012-0067**, **CVE-2012-0066**

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malicious dump file.

Users of Wireshark should upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of Wireshark must be restarted for the update to take effect.

4.345.2. RHEA-2011:1772 — wireshark enhancement update

An updated wireshark package that provides one enhancement is now available for Red Hat Enterprise Linux 6.

Wireshark, previously known as Ethereal, is a network protocol analyzer. It is used to capture and browse the traffic running on a computer network.

Enhancement

BZ#746839

Prior to this update, Wireshark did not show traffic information for the Network File System (NFS) version 4.1 protocol. With this update, the NFS packet dissector is enhanced so that Wireshark correctly displays traffic for this protocol. Note that NFS version 4.1 is introduced as a Technology Preview for Red Hat Enterprise Linux 6.

Users of wireshark are advised to upgrade to this updated package, which adds this enhancement.

4.346. WPA_SUPPLICANT

4.346.1. RHEA-2011:1611 — wpa_supplicant enhancement update

An enhanced wpa_supplicant package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The wpa_supplicant package contains a WPA (Wi-Fi Protected Access) Supplicant utility for Linux, BSD, and Windows with support for WPA and WPA2 (IEEE 802.11i/RSN). The supplicant is a IEEE 802.1X/WPA component that is used in client workstations. It implements key negotiation with a WPA Authenticator and it controls the roaming and IEEE 802.11 authentication/association of the wlan driver.

The wpa_supplicant package has been upgraded to upstream version 0.7.3. This update provides the nl80211 driver and background scanning functionality that are required for efficient connections to RSA token-based WiFi networks. (BZ#713280)

Users that require roaming in RSA token-based WiFi networks are advised to upgrade to this updated package, which adds this enhancement.

4.347. X.ORG

4.347.1. RHBA-2011:1613 — X.Org support packages bug fix and enhancement update

Updated libpciaccess, xorg-x11-font-utils, xorg-x11-util-macros, xorg-x11-proto-devel and libdrm packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

These X.Org support packages are part of the platform necessary to run the latest X.Org server and drivers.

The libpciaccess library provides portable PCI access routines across multiple operating systems.

The Direct Rendering Manager runtime library (libdrm) provides a user-space interface library for direct rendering clients.

The xorg-x11-font-utils package provides X.Org X11 font utilities required for font installation, conversion and generation.

The xorg-x11-util-macros package provides X.Org X11 autotools macros required for building various packages that comprise the X Window System.

The xorg-x11-proto-devel package provides X.Org X11 Protocol headers.

The following packages have been upgraded to the higher upstream versions, which provide a number of bug fixes and enhancements over the previous versions:

BZ#713771

The libpciaccess package has been upgraded to upstream version 0.12.1.

BZ#713770

The libdrm package has been upgraded to upstream version 2.4.25.

BZ#717022

The xorg-x11-font-utils package has been upgraded to upstream version 7.2.

BZ#713846

The xorg-x11-util-macros package has been upgraded to upstream version 1.14.0.

BZ#713845

The xorg-x11-proto-devel package has been upgraded to upstream version 7.6.

Bug Fix

BZ#747965

The file permissions were set incorrectly for certain device nodes, such as the /dev/dri/controlD64 file. This problem could have been misused for DoS (Denial of Service) attacks against the current console users if the users were running X Windows. With this update, the file permissions are now set more strictly for these device nodes.

All users of libpciaccess, xorg-x11-font-utils, xorg-x11-util-macros, xorg-x11-proto-devel and libdrm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.347.2. RHEA-2011:1592 — X.Org X11 input drivers enhancement update

Updated xorg-x11-drv-acecad, xorg-x11-drv-aiptek, xorg-x11-drv-elographics, xorg-x11-drv-fpit, xorg-x11-drv-hyperpen, xorg-x11-drv-evdev, xorg-x11-drv-void, xorg-x11-drv-vmmouse, xorg-x11-drv-mouse, xorg-x11-drv-keyboard, xorg-x11-drv-synaptics, xorg-x11-drv-mutouch, and xorg-x11-drv-penmount packages that add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-keyboard and xorg-x11-drv-mouse packages contain the legacy X.Org X11 input drivers for keyboards and mice.

The xorg-x11-drv-acecad, xorg-x11-drv-aiptek, xorg-x11-drv-hyperpen, xorg-x11-drv-elographics, xorg-x11-drv-fpit, xorg-x11-drv-mutouch, xorg-x11-drv-penmount, xorg-x11-drv-evdev, xorg-x11-drv-vmmouse, and xorg-x11-drv-synaptics packages contain the X.Org X11 input drivers for legacy devices.

BZ#713777

The xorg-x11-drv-acecad package has been upgraded to upstream version 1.5.0.

BZ#713778

The xorg-x11-drv-aiptek package has been upgraded to upstream version 1.4.1.

BZ#713783

The xorg-x11-drv-elographics package has been upgraded to upstream version 1.3.0.

BZ#713788

The xorg-x11-drv-fpit package has been upgraded to upstream version 1.4.0.

BZ#713802

The xorg-x11-drv-hyperpen package has been upgraded to upstream version 1.4.1.

BZ#713786

The xorg-x11-drv-evdev package has been upgraded to upstream version 2.6.0.

BZ#713841

The xorg-x11-drv-vmmouse package has been upgraded to upstream version 12.7.0.

BZ#713809

The xorg-x11-drv-mouse package has been upgraded to upstream version 1.7.0.

BZ#713807

The xorg-x11-drv-keyboard package has been upgraded to upstream version 1.6.0.

BZ#713861

The xorg-x11-drv-synaptics package has been upgraded to upstream version 1.4.1.

BZ#713810

The xorg-x11-drv-mutouch package has been upgraded to upstream version 1.3.0.

BZ#713812

The xorg-x11-drv-penmount package has been upgraded to upstream version 1.5.0.

All users of these packages are advised to upgrade to these updated packages, which provide a number of enhancements over the previous versions.

4.347.3. RHEA-2011:1601 — X.Org video driver packages bug fix and enhancement update

Updated xorg-x11-drv-apm, xorg-x11-drv-ast, xorg-x11-drv-cirrus, xorg-x11-drv-dummy, xorg-x11-drv-fbdev, xorg-x11-drv-geode, xorg-x11-drv-glint, xorg-x11-drv-i128, xorg-x11-drv-i740, xorg-x11-drv-mach64, xorg-x11-drv-neomagic, xorg-x11-drv-nv, xorg-x11-drv-openchrome, xorg-x11-drv-r128, xorg-x11-drv-rendition, xorg-x11-drv-s3virge, xorg-x11-drv-savage, xorg-x11-drv-siliconmotion, xorg-x11-drv-sis, xorg-x11-drv-sisusb, xorg-x11-drv-tdfx, xorg-x11-drv-trident, xorg-x11-drv-v4l, xorg-x11-drv-vesa, xorg-x11-drv-vmware, xorg-x11-drv-voodoo, xorg-x11-drv-xgi packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

These X.Org video driver packages provide video drivers needed for various graphics cards to work properly in the X.Org implementation of the X Window System.

The following packages have been upgraded to the higher upstream versions, which provide a number of bug fixes and enhancements over the previous versions:

BZ#713779

The xorg-x11-drv-apm package has been upgraded to upstream version 1.2.3.

BZ#713867

The xorg-x11-drv-ast package has been upgraded to upstream version 0.91.10.

BZ#713780

The xorg-x11-drv-cirrus package has been upgraded to upstream version 1.3.2.

BZ#713781

The xorg-x11-drv-dummy package has been upgraded to upstream version 0.3.4.

BZ#713787

The xorg-x11-drv-fbdev package has been upgraded to upstream version 0.4.2.

BZ#713789

The xorg-x11-drv-geode package has been upgraded to upstream version 2.11.12.

BZ#713790

The xorg-x11-drv-glint package has been upgraded to upstream version 1.2.5.

BZ#713803

The xorg-x11-drv-i128 package has been upgraded to upstream version 1.3.4.

BZ#713805

The xorg-x11-drv-i740 package has been upgraded to upstream version 1.3.2.

BZ#713808

The xorg-x11-drv-mach64 package has been upgraded to upstream version 6.9.0.

BZ#713811

The xorg-x11-drv-neomagic package has been upgraded to upstream version 1.2.5.

BZ#713855

The xorg-x11-drv-nv package has been upgraded to upstream version 2.1.18.

BZ#713856

The xorg-x11-drv-openchrome package has been upgraded to upstream version 0.2.904.

BZ#713813

The xorg-x11-drv-r128 package has been upgraded to upstream version 6.8.1.

BZ#713814

The xorg-x11-drv-rendition package has been upgraded to upstream version 4.2.4.

BZ#713832

The xorg-x11-drv-s3virge package has been upgraded to upstream version 1.10.4.

BZ#713833

The xorg-x11-drv-savage package has been upgraded to upstream version 2.3.2.

BZ#713835

The xorg-x11-drv-siliconmotion package has been upgraded to upstream version 1.7.5.

BZ#713859

The xorg-x11-drv-sis package has been upgraded to upstream version 0.10.3.

BZ#713836

The xorg-x11-drv-sisusb package has been upgraded to upstream version 0.9.4.

BZ#713837

The xorg-x11-drv-tdfx package has been upgraded to upstream version 1.4.3.

BZ#713838

The xorg-x11-drv-trident package has been upgraded to upstream version 1.3.4.

BZ#713839

The xorg-x11-drv-v4l package has been upgraded to upstream version 0.2.0.

BZ#713840

The xorg-x11-drv-vesa package has been upgraded to upstream version 2.3.0.

BZ#713842

The xorg-x11-drv-vmware package has been upgraded to upstream version 11.0.3.

BZ#713844

The xorg-x11-drv-voodoo package has been upgraded to upstream version 1.2.4.

BZ#713860

The xorg-x11-drv-xgi package has been upgraded to upstream version 1.6.0.

Bug Fix

BZ#704094

Due to a missing XGIPowerSaving() function call in the xgi video driver's source code, a server using XGI Z9-series graphics chipset was not able to recover from power-saving mode. With this update, the XGIPowerSaving() function call has been added and the server now recovers properly.

All users of these X.Org video driver packages are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.348. XDG-UTILS

4.348.1. RHBA-2011:1229 — xdg-utils bug fix update

An updated xdg-utils package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The xdg-utils package is a set of simple scripts that provide basic desktop integration functions for any Free Desktop.

Bug Fixes

BZ#659782

Previously, a trailing comma was passed in the "thunderbird" command. As a result, Thunderbird was unable to open a compose window. With this update, the trailing comma has been stripped so that Thunderbird now works properly.

BZ#659786

Previously, there was a typo found in the xdg-utils source code. As a consequence, Thunderbird, after passing in an email address, created a compose window without the "To:" address. With this update, the typo has been fixed so that the "To:" address is now passed in correctly.

All xdg-utils users are advised to upgrade to this updated package, which fixes these bugs.

4.349. XFSPROGS

4.349.1. RHBA-2011:1736 — xfsprogs bug fix update

Updated xfsprogs packages that fix two bugs are now available.

xfsprogs contains a set of commands to use the XFS filesystem, including mkfs.xfs.

Bug Fixes

BZ#679154

xfs_quota is the xfsprogs utility for managing XFS file system quotas. When "xfs_quota" was run on an XFS file system which had user quotas enabled but no enabled group quotas, it generated "XFS_GETQUOTA: No such process" errors. That is, xfs_quota was asking for and attempting to report on quotas which were not there. This update corrects this behavior. xfs_quota no longer tries to report on quotas that are not present and, consequently, the error above no longer presents.

BZ#694706

xfs_repair is the xfsprogs utility for repairing XFS file systems. Previously, when "xfs_repair -n" (the "-n" switch puts xfs_repair into "report-only, do not modify" mode) was run on an XFS filesystem, a check for whether a particular called pointer -- agno -- was within the file system was not done. In some circumstances (for example, if the file system had corrupted directory entries) this could cause the utility to read uninitialized memory, resulting in a segfault. As of this update "xfs_mount" is specifically passed to affected functions and agno is checked to ensure it is inside the XFS file system. Consequently, the uninitialized memory reads and resultant segfaults no longer occur.

All XFS users should upgrade to these updated packages, which resolve these issues.

4.350. XINETD

4.350.1. RHBA-2012:1161 — xinetd bug fix update

An updated xinetd package that fixes one bug is now available for Red Hat Enterprise Linux 6 Extended Update Support.

Xinetd is a secure replacement for inetd, the Internet services daemon. Xinetd provides access control for all services based on the address of the remote host and/or on time of access, and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and allows users to bind specific services to specific IP addresses on a host machine. Each service has its own specific configuration file for Xinetd; the files are located in the /etc/xinetd.d directory.

Bug Fix

BZ#841915

Due to incorrect handling of a file descriptor array in the service.c source file, some of the descriptors remained open when xinetd was under heavy load. Additionally, the system log was filled with a large number of messages that took up a lot of disk space over time. This bug has been fixed in the code, xinetd now handles the file descriptors correctly and no longer fills the system log.

All users of xinetd are advised to upgrade to this updated package, which fixes this bug.

4.350.2. RHBA-2011:1713 — xinetd bug fix update

An updated xinetd package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The xinetd daemon is a secure replacement for inetd, the Internet services daemon. It provides access control for all services based on the address of the remote host and/or on time of access, and can prevent denial of service (DoS) attacks.

Bug Fixes

BZ#706976

Previously, the configuration files of the xinetd utility were readable for all users. This update makes the permissions more restrictive and the configuration files are now readable only by root.

BZ#738662

Previously, the /etc/xinet.d/ directory was owned by both the filesystem and xinetd packages. This bug has been fixed, and the directory is now owned only by the filesystem package.

Users of xinetd are advised to upgrade to this updated package which fixes these bugs.

4.351. XKEYBOARD-CONFIG

4.351.1. RHBA-2011:1591 — xkeyboard-config bug fix and enhancement update

An updated xkeyboard-config package that fixes one bug and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The xkeyboard-config package provides the xkeyboard-config alternative xkb data files.

Bug Fix

BZ#638612

Prior to this update, duplicate mapping for the backslash key caused the Indic Onscreen Keyboard (IOK) to exit with a segmentation fault when the Hindi Wx mapping was selected. This update modifies the mapping so that IOK no longer exits unexpectedly.

Enhancements

BZ#651774

With this update, the Unicode Rupee symbol is now included in the Indic keyboard layouts.

BZ#713863

This update upgrades the xkeyboard-config data files to upstream version 2.3.

All users of xkeyboard-config are advised to upgrade to this updated package, which addresses this bug and adds these enhancements.

4.352. XORG-X11-DRV-ATI

4.352.1. RHBA-2011:1553 — xorg-x11-drv-ati bug fix and enhancement update

Updated xorg-x11-drv-ati packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-ati packages provide a driver for ATI graphics cards for the X.Org implementation of the X Window System.

The xorg-x11-drv-ati packages have been upgraded to upstream version 6.14.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#713766, BZ#634238)

Bug Fixes

BZ#588918

The ATI ES1000 graphics devices had limited Video RAM (VRAM) and were restricted to an 8-bit color depth for the text console. As a consequence, the graphical boot screen was unavailable on systems using these graphics devices. Such systems could become unresponsive afterward and had to be rebooted. With this update, the source code is modified and the installation with graphical user interface (GUI) can be successfully completed.

BZ#615550

Due to the driver being too verbose, error messages about failed write attempts could incorrectly appear when booting the system on i386 architectures. The messages could be safely ignored and the system eventually booted successfully. To avoid user confusion, these messages are removed with this update.

Enhancements

BZ#675297

This update adds support for the AMD FirePro M5950, AMD FirePro M8900, AMD FirePro V5900, and AMD FirePro V7900 graphics cards.

BZ#713622

This update provides the firmware files which are required by AMD Radeon HD 6000-series and AMD's Accelerated Processing Unit (APU) platforms.

All users of xorg-x11-drv-ati are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.353. XORG-X11-DRV-INTEL

4.353.1. RHBA-2011:1619 — xorg-x11-drv-intel bug fix and enhancement update

Updated xorg-x11-drv-intel packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-intel packages contain an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

The xorg-x11-drv-intel packages have been upgraded to upstream version 2.16, which provides a number of bug fixes and enhancements over the previous version. (BZ#713767)

Bug Fixes

BZ#699933

A black screen could appear when attempting to turn on a Lenovo ThinkPad T500 laptop after suspending it. As a consequence, the laptop could not recover from suspend. The source code has been modified so that Lenovo ThinkPad T500 laptops now recover from suspend successfully.

BZ#720702

Prior to this update, arithmetic rounding in the panel fitting algorithm did not work as expected. As a result, the screen was staggered in a diagonal way when scaling up the 1360x768 mode for the Intel Ironlake driver with Low-voltage differential signaling (LVDS) while the scaling mode was set to "None" or "Full aspect". This update modifies the rounding in the panel fitting algorithm so that the screen resolution can now be changed correctly.

Enhancement

BZ#684313

This update adds support for future Intel embedded graphics controllers and enables additional 3D features.

All users of xorg-x11-drv-intel are advised to upgrade to these updated xorg-x11-drv-intel packages, which fix these bugs and add this enhancement.

4.354. XORG-X11-DRV-MGA

4.354.1. RHBA-2011:1620 — xorg-x11-drv-mga bug fix and enhancement update

Updated xorg-x11-drv-mga packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-mga packages porvide a video driver for Matrox G-series chipsets for the X.Org implementation of the X Window System.

The xorg-x11-drv-mga packages have been upgraded to upstream version 1.4.13, which provides a number of bug fixes over the previous version. (BZ#713858)

Bug Fixes

BZ#713388

Previously, the MGA driver rendered the image incorrectly on big-endian architectures, including PowerPC and 64-bit PowerPC. Consequently, the display showed altered colors. With this update, the colors are displayed correctly in the described scenario.

BZ#745080

Previously, the MGA driver caused a shift in the video screen. Consequently, the screen became corrupted and the windows were pushed around randomly. This update, modifies the code so that the MGA driver no longer causes problems for the video screen.

Enhancement

BZ#526104

This update adds support for ServerEngines Pilot III to the xorg-x11-drv-mga packages.

All users of the Xorg x11 MGA driver, are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.355. XORG-X11-DRV-NOUVEAU

4.355.1. RHBA-2011:1600 — xorg-x11-drv-nouveau bug fix and enhancement update

Updated xorg-x11-drv-nouveau packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-nouveau utility provides the Xorg X11 Nouveau video driver for NVIDIA graphics chipsets.

Bug Fix

BZ#708500

Prior to this update, one process was used to scan for all defects. As a result, xorg-x11-drv-nouveau packages did not build without patches against its supporting components. This update scans defects in downstream patches separately. Now, the packages build as expected when not all downstream patches are present.

Enhancement

BZ#713768

This update adds the updated Xorg Nouveau driver for NVIDIA GeForce/Quadro hardware to the xorg-x11-drv-nouveau package.

All users of the Xorg x11 Nouveau driver, are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

4.356. XORG-X11-DRV-QXL

4.356.1. RHEA-2011:1621 — xorg-x11-drv-qxl bug fix and enhancement update

An updated xorg-x11-drv-qxl package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-qxl package provides an X11 video driver for the QEMU QXL video accelerator. This driver makes it possible to use Red Hat Enterprise Linux 6 as a guest operating system under the KVM kernel module and the QEMU multi-platform emulator, using the SPICE protocol.

The xorg-x11-drv-qxl package has been upgraded to upstream version 0.0.14, which provides a number of bug fixes and enhancements over the previous version. BZ#713857

All users of xorg-x11-drv-qxl are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.356.2. RHBA-2012:0380 — xorg-x11-drv-qxl bug fix update

An updated xorg-x11-drv-qxl package that fixes two bug is now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-qxl package provides an X11 video driver for the QEMU QXL video accelerator. This driver makes it possible to use Red Hat Enterprise Linux 6 as a guest operating system under the KVM kernel module and the QEMU multi-platform emulator, using the SPICE protocol.

Bug Fixes

BZ#794877

The QXL driver for Red Hat Enterprise Linux 6.2 did not contain the compatibility layer. As a consequence, updating a Red Hat Enterprise Linux 6 guest running on a Red Hat Enterprise Linux 5 host in the Red Hat Enterprise Virtualization 2.2 environment caused the SPICE client window to become black after the update, and therefore unusable. A patch has been applied to ensure proper compatibility and the driver now works correctly in the described scenario.

BZ#799524

The QXL driver for Red Hat Enterprise Linux 6.2 was not able to cache images on the client side. This led to visible and significant impact on user experience (users could have experienced delays when loading images contained in web presentations or slideshows). With this update, images can be optionally cached on the client side.

All users of xorg-x11-drv-qxl are advised to upgrade to this updated package, which fixes these bugs.

4.357. XORG-X11-DRV-WACOM AND WACOMCPL

4.357.1. RHBA-2011:1588 — xorg-x11-drv-wacom and wacomcpl bug fix and enhancement update

Updated xorg-x11-drv-wacom and wacomcpl packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-wacom package provides an X Window System input device driver that allows the X server to handle Wacom tablets with extended functionality.

The wacomcpl package provides a graphical user interface (GUI) for the xorg-x11-drv-wacom X input device driver.

The wacomcpl package has been upgraded to upstream version 0.10, which provides a number of bug fixes and enhancements over the previous version. (BZ#713864)

Bug Fixes

BZ#713769

With this update, the new X.Org server is now supported.

BZ#641759

Previously, the xsetwacom(1) manual page contained a typographical error. This update corrects the typographical error.

BZ#675672

Previously, calibration could be inaccurate when using TwinView while the orientation was set to "LeftOf". With this update, the source code is modified and calibration now works as expected.

Enhancements

BZ#711618

Prior to this update, the wacomcpl utility supported only a single wacomcplrc file in the user's home directory. All the user settings were restored from this file when logging in. When various users logged into multiple machines with a different setup, a user had to update the wacomcplrc file every time. With this update, wacomcpl is modified to support host-specific wacomcplrc files. If no file exists with a hostname suffix, wacomcpl finally tries to load the wacomcplrc file without the suffix.

BZ#711619

With this update, the eraser automatically updates to the same calibration setting as the stylus when calibrating or binding the stylus to a screen using wacomcpl.

All users of xorg-x11-drv-wacom and wacomcpl are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.358. XORG-X11-SERVER

4.358.1. RHBA-2011:1816 — xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix one bug are now available for Red Hat Enterprise Linux 6.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Bug Fix

BZ#759022

Previously, a bug in Xephyr's input handling code disabled screens on a screen crossing event.

When the Xephyr nested X server was configured in a multi-screen setup, the focus was only on the screen where the mouse was located, and only this screen was updated. The aforementioned code has been removed and the Xephyr server now correctly updates screens in multi-screen setups.

All users of xorg-x11-server are advised to upgrade to these updated packages, which fix this bugs.

4.358.2. RHBA-2012:0368 — xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix one bug are now available for Red Hat Enterprise Linux 6.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Bug Fix

BZ#783505

Previously, if the X server was configured as a multi-screen setup through multiple "Device" sections in the xorg.conf file, an absolute input device (for example a graphic tablet's stylus) got stuck in the right-most or bottom-most screen. This update changes the screen crossing behavior so that absolute devices are always mapped across all screens.

All users of xorg-x11-server are advised to upgrade to these updated packages, which fix this bug.

4.359. XORG-X11-SERVER AND TIGERVNC

4.359.1. RHEA-2011:1602 — xorg-x11-server and tigervnc bug fix and enhancement update

Updated xorg-x11-server and tigervnc packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-server packages provide the X.Org sample implementation of a server for the X Window System. It provides the rendering services necessary for graphical user environments, such as GNOME and KDE.

The tigervnc packages provide a TigerVNC remote display system, which allows users to manage graphical applications on remote machines.

The xorg-x11-server packages have been upgraded to upstream version 1.10.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#506345)

Bug Fixes

BZ#740581

Due to a problem in the gnome-screensaver application that caused screen resume failures, the X server was set to stop proxying the lid state in output connectivity. As a consequence, when using certain configurations, such as a dual head setup with span mode, the screen configuration was not changed to use only the external screen on the laptop lid close. With this update, the problem with gnome-screensaver has been resolved, and X server has been modified to inspect the lid state again. When the laptop lid is closed, the laptop display is disconnected and the screen configuration is changed to use only the external monitor. When the laptop lid is open, the screen configuration returns to the dual head setup using span mode.

BZ#693793

The /usr/bin/xvfb-run script incorrectly used the undefined tempfile variable instead of the mktemp command when creating a temporary directory for an X authorization file. The script was not able to create the directory and therefore failed to start Xvfb (X virtual framebuffer). The xvfb-run script now works as expected using mktemp.

BZ#734262

The X server did not respect screen limits properly. Therefore, the mouse cursor could be moved outside the visible areas of the screen. Screen limits are now respected by the X server, and the cursor can no longer leave the visible areas of the screen.

BZ#740190

The X server did not recognize the lid state correctly if a laptop with attached external display booted with the lid closed. Therefore, the Gnome Display Manager's login dialog did not appear on the external screen. With this update, the X server recognizes the lid as closed, and the login dialog now displays on the external screen in the scenario described.

BZ#664484

Under certain circumstances, a user's keyboard and key mappings could go out of sync if the mappings were modified with the xmodmap utility. With this update, the underlying code has been fixed, and modified key mappings can now be used as expected.

BZ#655212

The panning feature did not work correctly with X Resize, Rotate and Reflect Extension (RandR) when CRTC cursor confinement was enabled. As a consequence, users were not able to move the mouse pointer beyond the visible part of the screen although certain inaccessible regions were within the panning area. With this update, RandR has been modified to disable CRTC cursor confinement when panning is enabled. The panning feature now works as expected.

BZ#664927

When the XChangePointerControl() function was called by a driver after a device was removed from the system, the function tried to dereference the pointer to already freed memory. As a consequence, the X server terminated with a segmentation fault. The X server does not call this function anymore and crashes no longer in the situation described.

BZ#734969

Pointer events were not handled correctly when switching screens using the PointerKeys feature with multi-head ATI or NVIDIA graphics cards. This caused the X server to terminate unexpectedly. With this update, events handling has been modified and the X server no longer crashes under these circumstances.

All users of xorg-x11-server and tigervnc are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.360. XORG-X11-SERVER-UTILS

4.360.1. RHBA-2011:1617 — xorg-x11-server-utils bug fix and enhancement update

Updated xorg-x11-server-utils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-server-utils package contains a collection of utilities used to modify and query the runtime configuration of the X.Org server. X.Org is an open source implementation of the X Window System.

The xorg-x11-server-utils packages have been upgraded to upstream version 7.1 which provides a number of bug fixes and enhancements over the previous version. (BZ#713862)

Bug Fixes

BZ#657554

Previously, the xrandr options --scale and -- transform caused a segmentation fault, because these options required an --output field but the utility didn't validate the command line properly check for existing output. With this update, xrandr displays a message informing that the --scale and -- transform options also require the --output option.

BZ#740146

Previously, xrandr wrongly assumed that a gamma ramp value of zero was a failure. When VNC was enabled, xrandr returned a zero value. With this update, xrandr is modified to allow for a gamma ramp value of zero. Now xrandr no longer fails when running VNC.

All users of xorg-x11-server-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.361. XULRUNNER

4.361.1. RHSA-2012:0143 — Critical: xulrunner security update

Updated xulrunner packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

XULRunner provides the XUL Runtime environment for applications using the Gecko layout engine.

Security Fix

CVE-2011-3026

A heap-based buffer overflow flaw was found in the way XULRunner handled PNG (Portable Network Graphics) images. A web page containing a malicious PNG image could cause an application linked against XULRunner (such as Firefox) to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

All XULRunner users should upgrade to these updated packages, which correct this issue. After installing the update, applications using XULRunner must be restarted for the changes to take effect.

4.362. YABOOT

4.362.1. RHBA-2011:1767 — yaboot bug fix update

An updated yaboot package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The yaboot package provides a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

Bug Fixes

BZ#638654

Previously, yaboot could not check whether an IP address is valid. As a consequence, yaboot netboot failed to operate in an environment where the gateway was not the same as the 'tftp' server, even though the 'tftp' server was on the same subnet. With this update, an IP address validity check has been added. Now,yaboot netbot operates as expected.

BZ#746340

Previously, yaboot discarded passed parameters to anaconda after the Client Architecture Support (CAS) was rebooted. This update upgrades the yaboot binary and modifies the source file. Now, the parameters are passed to the anaconda installer as expected.

All users of yaboot are advised to upgrade to this updated package, which fixes these bugs.

4.363. YP-TOOLS

4.363.1. RHEA-2011:1561 — yp-tools enhancement update

An enhanced yp-tools package that provides an enhancement is now available for Red Hat Enterprise Linux 6.

The Network Information Service (NIS) is a system which provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can enable users to login on any machine on the network as long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP).

Enhancement

BZ#699666

When using the passwd.adjunct file, the ypasswd client program did not recognize the salt used for hashing a new password and therefore chose DES as the default hash function. A new environment variable YP_PASSWD_HASH, which allows users to choose the hash algorithm, was added.

Users of yp-tools are advised to upgrade to this updated package, which adds this enhancement.

4.364. YPSERV

4.364.1. RHBA-2011:1557 — ypserv bug fix and enhancement update

An updated ypserv package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The ypserv utility provides network information (login names, passwords, home directories, group

information) to all of the machines on a network. It can enable users to log in on any machine on the network as long as the machine has the Network Information Service (NIS) client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP).

Bug Fixes

BZ#699675

Uninitialized memory could be accessed when running the "yppasswdd" command with the "-x" option to pass data to an external program. As a consequence, redundant characters were prefixed to the request string, which led to incorrect parsing of the request. This update fixes the memory initialization and the request can be now parsed successfully.

BZ#734494

Prior to this update, the root user could see old passwords of other users. This was caused by a change request being logged using syslog when running the "yppaswdd" command with the "-x" option to pass data to an external program. With this update, the old password hash and the new password hash are cleared in syslog and the root user can no longer view the old passwords of other users.

Enhancement

BZ#699667

Prior to this update, users were not able to change their passwords by running the "yppasswd" command if using the passwd.adjunct file, which prevents disclosing the encrypted passwords. With this update, users are now able to change their passwords.

All users of ypserv are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.365. YUM

4.365.1. RHBA-2011:1702 — yum bug fix and enhancement update

An updated yum package that fixes several bugs and adds three enhancements is now available for Red Hat Enterprise Linux 6.

Yum is a command line utility that allows a user to check for and automatically download and install updated RPM packages. It automatically obtains and downloads dependencies, prompting the user for permission as necessary.

Bug Fixes

BZ#661962

When uninstalling a package, the "yum remove" command may have previously reported success even when the package could not be removed due to an error in the %pre scriptlet. With this update, this error has been fixed, and when yum fails to remove a package, it no longer claims that it succeeded.

BZ#697885

When running the "yum -v repolist" command, the previous version of the yum utility may have incorrectly displayed a duplicate "Repo-baseurl" line for a repository with no mirrors. This update

applies a patch that corrects this error, and the output of the "yum -v repolist" command no longer contains duplicate lines.

BZ#704600

Previously, an attempt to install a package that was larger than 4 GB on a 32-bit architecture caused yum to terminate unexpectedly with a traceback. With this update, the underlying source code has been adapted to work around this problem, and packages larger than 4 GB can now be installed as expected.

BZ#707358

Prior to this update, running a yum command with the "--installroot" command line option caused it to report the following warning:

```
Ignored option -c (probably due to merging -yc != -y -c)
```

This update adapts the underlying source code not to display this warning when the "--installroot" option is in use, resolving this issue.

BZ#727574

Under certain circumstances, an attempt to use the RepoStorage API may have failed with an AttributeError. With this update, this error has been fixed, and the RepoStorage API can now be used as expected.

BZ#727586

Previously, the repodiff utility used a stale metadata cache in subsequent runs. When two repodiff commands were executed in succession, the second run reused cached data from the first. This bug has been fixed and repodiff now properly validates the metadata if a connection cannot be established or the cached data are about to be reused.

BZ#728253

Prior to this update, when the "yum -q history addon-info last saved_tx" command was used to store transaction data in a file, an attempt to supply this file to the "yum load-transaction" command in order to repeat the transaction failed with an error, because the output contained extra lines. This update corrects the underlying source code to make sure the "yum -q history addon-info last saved_tx" command produces valid output, and adapts "yum load-transaction" to accept older version of the output as well.

BZ#733391

In very rare cases, the yum utility may have incorrectly kept using old updateinfo, pkgtags, and groups metadata. When this happened, users may have been unaware of available updates for up to 6 hours. This update applies a patch that prevents yum from using outdated metadata, resolving this issue.

Enhancements

BZ#662243

The "yum history" command has been adapted to store and display yumdb and rpmdb information, such as from which repository was a particular package installed.

BZ#728526

The "yum update" command can now be used to update a package to a specific version.

BZ#694401

The yum utility no longer asks the user to report a bug when the dependency solver (depsolve) encounters an error.

All users of yum are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.365.2. RHBA-2012:0386 — yum bug fix update

An updated yum package that fixes one bug is now available for Red Hat Enterprise Linux 6.

Yum is a command line utility that allows the user to check for updates and automatically download and install updated RPM packages. Yum automatically obtains and downloads dependencies, prompting the user for permission as necessary.

Bug Fix

BZ#795455

The anacron scheduler starts the yum-cron utility with the "nice" value of 10. This caused Yum's RPM transactions to run at very low priority level. Also, any updated service inherited this "nice" value, which influenced the system behavior. This update adds the "reset_nice" configuration option, which allows Yum to reset the "nice" value to 0 before running an RPM transaction. With this option set, Yum's RPM transactions run at normal priority level so that updated services are restarted with normal priority as expected.

All users of yum are advised to upgrade to this updated package, which fixes this bug.

4.366. YUM-UTILS

4.366.1. RHBA-2011:1703 — yum-utils bug fix and enhancement update

Updated yum-utils packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The yum-utils packages provide a collection of utilities and examples for the Yum package manager.

Bug Fixes

BZ#694188

When using the previous version of the yum-groups-manager utility, an attempt to use the "-c" (or "--config") command line option to specify an alternative configuration file failed, and the utility incorrectly used the default /etc/yum.conf file. This update adapts the underlying source code to correct this error, and yum-groups-manager now accepts alternative configuration files as expected.

BZ#699470

Prior to this update, when the yumdownloader utility failed to download a requested package, it incorrectly exited with a status of 0. With this update, yumdownloader exits with a non-zero status in these situations.

BZ#709043

Due to an error in the detection of the return value of an internal method, the previous version of the yum-builddep utility failed to exit with a non-zero exit status when it encountered an error. This update applies a patch that ensures the return value of the aforementioned method is correctly evaluated, and when an error is encountered, yum-builddep now exits with a non-zero status as expected.

BZ#713108

Previously, when a user executed the reposync utility with the "-r" (or "--repoid") command line option, the utility incorrectly used repositories that were enabled in the configuration. This update applies a patch to make sure these command line options work correctly.

BZ#734428

When using the priorities plug-in, running the "yum update" command may have incorrectly failed to offer some packages for update. This update corrects this error, and the priorities plug-in no longer prevents "yum update" from fully updating the system.

BZ#659740

Prior to this update, certain commands in the EXAMPLES sections of the repoquery(1), show-installed(1), yum-filter-data(1), yum-groups-manager(1), yum-list-data(1), and yum-verify(1) manual pages used incorrect glyphs for single quotes. Consequent to this, an attempt to copy such a command and run it on the command line failed with an error. This update ensures that all command examples now use typewriter straight single quotes as expected.

BZ#720967

Various typos in the yum-security(8) manual page have been corrected.

Enhancement

BZ#710469

Source repository patterns for Red Hat Network (RHN) have been added to the yumdownloader and yum-builddep utilities.

All users of yum-utils are advised to upgrade to these updated packages, which fix these bugs.

4.367. ZLIB

4.367.1. RHBA-2011:0931 — zlib bug fix update

Updated zlib packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The zlib package provides a general-purpose lossless data compression library that is used by many different programs.

Bug Fix

BZ#622781

When used to combine two Adler-32 checksums, the adler32_combine() function could have produced an incorrect result under certain circumstances. With this update, the underlying algorithm has been fixed, and the adler32_combine() function no longer returns incorrect checksums.

All users of zlib are advised to upgrade to these updated packages, which fix this bug.

4.367.2. RHEA-2011:1678 — zlib enhancement update

Enhanced zlib packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The zlib package provides a general-purpose lossless data compression library that is used by many different programs.

Enhancement

BZ#727288

This update sets RELRO flags by default, so that the zlib library is compiled with partial RELRO protection support.

All users of zlib are advised to upgrade to these updated packages, which add this enhancement.

4.368. CLUSTER

4.368.1. RHBA-2013:1054 — cluster and gfs2-utils bug fix update

Updated cluster and gfs2-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The Red Hat Cluster Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure. Using redundant hardware, shared disk storage, power management, and robust cluster communication and application failover mechanisms, a cluster can meet the needs of the enterprise market.

Bug Fix

BZ#982698

Previously, the cman init script did not handle its lock file correctly. During a node reboot, this could have caused the node itself to be evicted from the cluster by other members. With this update, the cman init script now handles the lock file correctly, and no fencing action is taken by other nodes of the cluster.

Users of cluster and gfs2-utils are advised to upgrade to these updated packages, which fix this bug.

4.369. DB4

4.369.1. RHBA-2013:1443 — db4 bug fix update

Updated db4 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Berkeley Database (Berkeley DB) is a programmatic toolkit that provides embedded database support for both traditional and client/server applications. The Berkeley DB includes B+tree, Extended Linear Hashing, Fixed and Variable-length record access methods, transactions, locking, logging, shared memory caching, and database recovery. The Berkeley DB supports C, C++, Java, and Perl APIs. It is used by many applications, including Python and Perl, so this should be installed on all systems.

Bug Fix

BZ#1012585

Due to an incorrect order of the mutex initialization calls, the rpm utility became unresponsive under certain circumstances, until it was terminated. With this update, the order of the mutex initialization calls has been revised. As a result, the rpm utility no longer becomes unresponsive.

Users of db4 are advised to upgrade to these updated packages, which fix this bug.

4.370. RPCBIND

4.370.1. RHBA-2013:1454 — rpcbind bug fix

Updated rpcbind packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The rpcbind utility maps RPC (Remote Procedure Call) services to the ports on which the services listen and allows the host to make RPC calls to the RPC server.

Bug Fix

BZ#858572

Previously, in the insecure mode, which enables non-root users to set or unset ports, a privileged port was required. As only root users can obtain a privileged port, non-root users could not set or unset ports. To fix this bug, the privileged port has been removed, and thus non-root users are now allowed to set or unset ports on the loopback interface.

All users of rpcbind are advised to upgrade to these updated packages, which fix this bug.

4.371. RSYNC

4.371.1. RHBA-2013:1485 — rsync bug fix update

An updated rsync package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The rsync tool is used to copy and synchronize files locally or across a network. The rsync works very fast because it uses delta encoding and sends just differences in files instead of whole files. The rsync is also used as powerful mirroring tool.

Bug Fix

BZ#1022355

Previously, the rsync tool did not check whether the inbuf variable is non-empty. As a consequence, rsync terminated unexpectedly while trying to do the required encoding in a loop. With this update, rsync checks whether inbuf is non-empty and no longer crashes in the described scenario.

Users of rsync are advised to upgrade to these updated packages, which fix this bug.

4.372. TZDATA

4.372.1. RHEA-2013:0674 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5 and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#921173, BZ#921174, BZ#919628, BZ#921176

Time zone rules of tzdata have been modified to reflect the following changes:

The period of Daylight Saving Time (DST) in Paraguay will end on March 24 instead of April 14.

Haiti will use US daylight-saving rules in the year 2013.

Morocco does not observe DST during Ramadan. Therefore, Morocco is expected to switch to Western European Time (WET) on July 9 and resume again to Western European Summer Time (WEST) on August 8.

Also, the tzdata packages now provide rules for several new time zones: Asia/Khandyga, Asia/Ust-Nera, and Europe/Busingen.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.372.2. RHEA-2013:1432 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1013527, BZ#1013875, BZ#1013876, BZ#1014720

Morocco extended DST by one month requiring an update to these packages. This update includes resynchronization with the latest upstream release in order to pick up the Moroccan DST change.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.372.3. RHEA-2013:0880 — tzdata enhancement update

Updated tzdata packages that add various enhancements are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancements

- The Gaza Strip and the West Bank entered Daylight Saving Time on March 28 at midnight local time. BZ#928461, BZ#928462, BZ#928463, BZ#928464

- Recent change to Daylight Saving rules in Paraguay appears to be perpetual. Transition times in years 2014 and later were updated accordingly.
- The Macquarie Island was uninhabited between years 1919 and 1948. This update introduces a new time type with a "zzz" abbreviation, which distinguishes uninhabited regions from the inhabited ones.
- The Macquarie Island belongs to Australia. This updated modifies the /usr/share/zoneinfo/zone.tab file accordingly.

All users of tzdata are advised to upgrade to these updated packages, which add these enhancements.

4.372.4. RHEA-2013:1025 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#980805, BZ#980807, BZ#981019, BZ#981020

Morocco does not observe DST during Ramadan. Therefore, Morocco is expected to switch to Western European Time (WET) on July 7 and resume again to Western European Summer Time (WEST) on August 10. Also, the period of DST in Israel has been extended until the last Sunday in October from the year 2013 onwards.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.372.5. RHEA-2013:0615 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5 and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#912521, BZ#916272, BZ#916273, BZ#916274

The Chilean Government is extending the period of Daylight Saving Time (DST) in the year 2013 until April the 27th. Then, Chile Standard Time (CLT) and Easter Island Standard Time (EAST) will be in effect until September the 7th when switching again to DST. With this update, the rules used for Chile time zones have been adjusted accordingly.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.373. RED HAT ENTERPRISE LINUX 6.2 EXTENDED UPDATE SUPPORT 6-MONTH NOTICE

4.373.1. RHSA-2013:1001 — Low: Red Hat Enterprise Linux 6.2 Extended Update Support 6-Month Notice

This is the 6-Month notification for the retirement of Red Hat Enterprise Linux 6.2 Extended Update Support (EUS).

In accordance with the Red Hat Enterprise Linux Errata Support Policy, Extended Update Support for Red Hat Enterprise Linux 6.2 will be retired on December 31, 2013, and support will no longer be provided. Accordingly, Red Hat will no longer provide updated packages, including critical impact security patches or urgent priority bug fixes, for Red Hat Enterprise Linux 6.2 EUS after that date. In addition, after December 31, 2013, technical support through Red Hat's Global Support Services will no longer be provided.

Note: This notification applies only to those customers subscribed to the Extended Update Support (EUS) channel for Red Hat Enterprise Linux 6.2.

We encourage customers to plan their migration from Red Hat Enterprise Linux 6.2 to a more recent version of Red Hat Enterprise Linux 6. As a benefit of the Red Hat subscription model, customers can use their active subscriptions to entitle any system on a currently supported Red Hat Enterprise Linux 6 release (6.3, or 6.4, for which EUS is available).

Details of the Red Hat Enterprise Linux life cycle can be found here:

https://access.redhat.com/support/policy/updates/errata/

APPENDIX A. REVISION HISTORY

Revision 1-6 **Wed Feb 25 2015** **Laura Bailey**

Rebuild for sort order.

Revision 1-5 **Wed Jan 21 2014** **Elišla Slobodová**

Added the missing eCryptfs Technology Preview.

Revision 1-4.6 **Tue Jun 18 2013** **Miroslav Svoboda**

Documented a new kernel erratum, RHSA-2013:1026.

Revision 1-4.5 **Tue Jun 18 2013** **Eliška Slobodová**

Fixed broken links and links pointing to the old Product Documentation site.

Revision 1-4.4 **Thu Nov 1 2012** **Eliška Slobodová**

Updated the initscripts known issue to provide a more detailed description of the problem.

Revision 1-2 **Tue Oct 2 2012** **Martin Prpič**

Removed “KVM Live Snapshots” from the list of Technology Previews. This feature is only available via Red Hat Enterprise Virtualization 3.0.

Revision 1-1 **Wed May 20 2012** **Martin Prpič**

Republished Technical Notes to update list of included advisories. For more information, refer to the Important note in the *Package Updates* chapter of this book.

Revision 1-0 **Tue Dec 6 2011** **Martin Prpič**

Initial release of the Red Hat Enterprise Linux 6.2 Technical Notes.