Red Hat Enterprise Linux 6

6.0 Technical Notes

Technical Release Documentation

Edition 1

Last Updated: 2025-01-15

Red Hat Enterprise Linux 6 6.0 Technical Notes

Technical Release Documentation
Edition 1

Red Hat Engineering Content Services

Legal Notice

Abstract

Red Hat Enterprise Linux 6.0 Technical notes provide details on various features shipped in Red Hat Enterprise Linux 6.0, as well as all known issues of this release.

Table of Contents

1. INSTALLER

The Red Hat Enterprise Linux installer (also known as anaconda) assists in the installation of Red Hat Enterprise Linux 6.

Installation on systems with multipath and non-multipath storage devices

Installation of Red Hat Enterprise Linux 6 on a system with multipath and non-multipath storage devices the automatic partitioning layout in the installer may create volume groups containing a mix of multipath and non-multipath devices, thus defeating the purpose of multipath storage.

Users are advised to either select only multipath or only non-multipath devices on the disk selection screen that appears after selecting automatic partitioning. Alternatively, users can select custom partitioning.

1.1. Known Issues

- *The following issue applies to IBM Power Systems only.*

  anaconda will not create a new PReP boot partition on the root disk when performing a new Red Hat Enterprise Linux 6 installation on a system that contains existing PReP Boot partitions that need to be preserved. Consequently, the Power SMS boot manager will be unable to boot the new Red Hat Enterprise Linux 6 installation. To work around this issue,

  1. Use the fdisk utility to temporarily change the partition type from type 41 'PReP Boot' to type 83 'Linux' for all existing Linux installations on the system.

  2. Perform the Red Hat Enterprise Linux 6 installation. During installation, a new PReP Boot partition will be created on the Red Hat Enterprise Linux 6 root disk.

  3. Post-installation, once the new Red Hat Enterprise Linux 6 installation is up and running, use the fdisk utility to restore all changed partition types to type 41 'PReP Boot'.

- Anaconda now utilizes **NetworkManager** for network interface configuration. Consequently, kickstart users that referenced the network settings located in **/tmp/netinfo** must now source the **ifcfg** files found in **/etc/sysconfig/network-scripts**

- In some circumstances, disks that contain a whole disk format (e.g. 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.

- The **nodmraid** boot parameter currently cannot be used to force installation on disks containing spurious BIOS RAID metadata. To work around this issue, boot into rescue mode and run the command **dmraid -rE /dev/sdX** on the disks in question. Alternatively, run **dd if=/dev/zero of=/dev/sdX** and let it process up until the end of the disk. Note, however that this alternate procedure may take longer to complete and will erase all data on the disk.

- Installation of Red Hat Enterprise Linux 6 on an IBM ThinkPad T43 notebook may appear to stall after choosing storage options. In these circumstances, the installer is attempting to interact with the floppy drive, and may be unresponsive for up to 30 minutes.

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

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

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

- Installation on large disks (i.e. more than 2TB) on non-EFI platforms may encounter some limitations. Many BIOS systems can only boot disks that contain MSDOS partition tables, which cannot fully address large disks. A GPT partition table can address the full disk, but may not be bootable from BIOS. Consequently, the Red Hat Enterprise Linux installer does not support installing the GRUB bootloader to disks that contain GPT partition tables on non-EFI systems. When installing Red Hat Enterprise Linux 6 on a non-EFI system that contains one or more large disks, create a GPT partition table on each of the disks before proceeding to the storage configuration portion of the install process. Leaving the large disks uninitialized, or using an MSDOS partition table on them, can cause problems when creating partitions using anaconda.

- Some Cisco UCS storage devices do not have UEFI support, which may lead to an unbootable Red Hat Enterprise Linux 6 system when installation is performed through virtual media with the system in "strict UCSM boot order rules" mode. Consequently, when installing using the UEFI method, after installation and reboot, the system will hang with a flashing cursor. To work around this issue, install the system using the BIOS install method as follows:

  1. Map the Red Hat Enterprise Linux 6 "boot.iso" file or entire OS DVD ISO using the virtual media tool
  2. Press F2 during boot to enter the BIOS setup screen
  3. Go to the "Boot Options" screen
  4. Change "UCSM boot order rules" to "Loose"
  5. Save settings and reboot
  6. Press F6 to access the boot device menu
  7. In the menu will be two options for the virtual media: "Cisco Virtual CD/DVD 1.20" and "EFI: Cisco Virtual CD/DVD 1.20 CDROM File1" select the first option to install using BIOS method. Note that only the first option will be present if using the "boot.iso" file, as it has no UEFI support.
  8. It may be necessary to re-order the devices in the BIOS Options screen after "Loose" mode has been selected in order to make the hard drive mapped to the system the first device in the boot order.

  The use of BIOS install method will effectively work around the bug, but will prevent booting from disks using a GPT partition table. This will restrict the size of disks usable as a boot disk.

- When installing on the s390x 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 installation, the installer will exit and installation will terminate.

- Multipath storage devices with serial numbers not exactly 16 or 32 characters in length will not be detected by anaconda during installation.

- Due to an issue with the shutdown sequence of the installer, Intel BIOS RAID sets might be left

in an unclean condition post installation. Consequently, they will be rebuilt during the first boot of the system after installation. Note that this issue has no impact other than a slower first boot up after installation.

- The installer currently does not support having the /boot volume on a logical volume. Consequently, when setting up mount points during installation, the /boot volume cannot be on an LVM volume. System z supports /boot on an LVM volume. In order to exploit this, manual configuration after installation is required. Refer to the zipl documentation for further information.

- Minimal installations lack NetworkManager, so users wishing to have network interfaces configured for use on the first boot after installation need to make sure the network interfaces are configured and the network service is enabled at boot time. The following kickstart commands will enable eth0 for DHCP and enable the 'network' service:

  ```
  network --device eth0 --onboot yes --bootproto dhcp
  services --enabled=network
  ```

  Refer to the network device configuration documentation for more details on what the ifcfg-ethX files may contain.

- 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.

- The anaconda partition editing interface includes a button labeled **Resize**. Note that you can only shrink a partition with this button, not enlarge a partition.

- System z installations cannot use the ext4 filesystem for the boot partition. The recommended alternative filesystem is ext3.

- Channel IDs(read, write, data) for network devices are required for defining and configuring network devices on s390 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.

- During an MPATH installation on IBM POWER 7 systems, a "DiskLabelCommit Error" might be returned. To work around this issue, first install the system in a single path configuration. Connect to the system via SSH, clear the partitions using the **fdisk -l** command, and delete the partitions, then exit the SSH session. Finally, continue the installation from the installer.

- anaconda in Red Hat Enterprise Linux 6 for Power writes an incorrect value to /etc/rpm/macros that can cause issues when installing 32 and 64-bit PowerPC packages together. Users are advised to remove this file after installation.

2. DEPLOYMENT

Upstart

In Red Hat Enterprise Linux 6, *init* from the sysvinit package has been replaced with *Upstart*, an event-based init system. This system handles the starting of tasks and services during boot, stopping them during shutdown and supervising them while the system is running. For more information on Upstart itself, refer to the **init(8)** man page.

Processes are known to Upstart as jobs and are defined by files in the **/etc/init** directory. Upstart is very well documented via man pages. Command overview is in **init(8)** and job syntax is described in **init(5)**.

Upstart provides the following behavioral changes in Red Hat Enterprise Linux 6:

- The **/etc/inittab** file is deprecated, and is now used *only* for setting up the default runlevel via the *initdefault* line. Other configuration is done via upstart jobs in the **/etc/init** directory.
- The number of active tty consoles is now set by the *ACTIVE_CONSOLES* variable in **/etc/sysconfig/init**, which is read by the **/etc/init/start-ttys.conf** job. The default value is *ACTIVE_CONSOLES=/dev/tty[1-6]*, which starts a getty on tty1 through tty6.
- A serial getty is still automatically configured if the serial console is the primary system console. In prior releases, this was done by **kudzu**, which would edit **/etc/inittab**. In Red Hat Enterprise Linux 6, configuration of the primary serial console is handled by **/etc/init/serial.conf**.
- To configure a getty running on a non-default serial console, you must now write an Upstart job instead of editing **/etc/inittab**. For example, if a getty on ttyS1 is desired, the following job file (**/etc/init/serial-ttyS1.conf**) would work:

```
# This service maintains a getty on /dev/ttyS1.

start on stopped rc RUNLEVEL=[2345]
stop on starting runlevel [016]

respawn
exec /sbin/agetty /dev/ttyS1 115200 vt100-nav
```

As in prior releases, you should still make sure that ttyS1 is in **/etc/securetty** if you wish to allow root logins on this getty.

There are some features from prior releases that are not supported in the move to Upstart. Among these are:

- Custom runlevels 7, 8 and 9. These custom runlevels can no longer be used.
- Using **/etc/shutdown.allow** for defining who can shut the machine down.

System z Performance

Some of the default tunables in Red Hat Enterprise Linux 6 are currently not optimally configured for System z workloads. Under most circumstances, System z machines will perform better using the following recommendations.

Dirty Ratio

It is recommended that the dirty ratio be set to 40 (Red Hat Enterprise Linux 6 default 20) Changing this tunable tells the system to not spend as much process time too early to write out dirty pages. Add the following line to /etc/sysctl.conf to set this tunable:

```
vm.dirty_ratio = 40
```

Scheduler

To increase the average time a process runs continuously and also improve the cache utilization and server style workload throughput at minor latency cost it is recommended to set the following higher values in /etc/sysctl.conf.

```
kernel.sched_min_granularity_ns = 10000000
kernel.sched_wakeup_granularity_ns = 15000000
kernel.sched_tunable_scaling = 0
kernel.sched_latency_ns = 80000000
```

Additionally, deactivating the Fair-Sleepers feature improves performance on a System z machine. To achieve this, set the following value in /etc/sysctl.conf

```
kernel.sched_features = 15834234
```

False positive hung task reports

It is recommended to prevent false positive hung task reports (which are rare, but might occur under very heavy overcommitment ratios). This feature can be used, but to improve performance, deactivate it by default by setting the following parameter in /etc/sysctl.conf:

```
kernel.hung_task_timeout_secs = 0
```

irqbalance service on the POWER architecture

On POWER architecture, the **irqbalance** service is recommended for automatic device Interrupt Request (IRQ) distribution across system CPUs to ensure optimal I/O performance. The **irqbalance** service is normally installed and configured to run during Red Hat Enterprise Linux 6 installation. However, under some circumstances, the **irqbalance** service is not installed by default. To confirm that the **irqbalance** service is running, execute the following command as root:

```
service irqbalance status
```

If the service is running, command will return a message similar to:

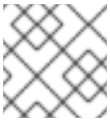
```
irqbalance (pid  1234) is running...
```

However, if the message lists the service as **stopped**, execute the following commands as root to start the irqbalance service:

```
service irqbalance start
chkconfig --level 345 irqbalance on
```

If the output of the **service irqbalance status** command lists irqbalance as an **unrecognized service**, use yum to install the irqbalance package, and then start the service.

```
yum install irqbalance
service irqbalance start
```



NOTE

The system does not need to be restarted after starting the irqbalance service

Setting the console log level

Use of the ***LOGLEVEL*** parameter in **/etc/sysconfig/init** to set the console loglevel is no longer supported. To set the console loglevel in Red Hat Enterprise Linux 6, pass '***loglevel=<number>***' as a boot time parameter.

Upgrading from previous pre-release versions

Upgrading to Red Hat Enterprise Linux 6 from Red Hat Enterprise Linux 5 or from previous pre-release versions of Red Hat Enterprise Linux 6 is not supported. If an upgrade of this type is attempted issues may be encountered including upgrading Java/OpenJDK packages. To work around this, manually remove the old packages and reinstall.

2.1. Known Issues

- When a system is configured to require smart card authentication, and there is no smartcard currently plugged into the system, then users might see the debug message:

  ```
  ERROR: pam_pkcs11.c:334: no suitable token available'
  ```

  This message can be safely ignored.

- Red Hat Enterprise Linux 6 Beta features Dovecot version 2.0. The configuration files used by Dovecot 2.0 are significantly different from those found in dovecot 1.0.x, the version shipped in previous releases of Red Hat Enterprise Linux. Specifically, **/etc/dovecot.conf** has been split into **/etc/dovecot/dovecot.conf** and **/etc/dovecot/conf.d/*.conf**

- Under some circumstances, the **readahead** service may cause the **auditd** service to stop. To work around this potential issue, disable the readahead collector by adding the following lines to the **/etc/sysconfig/readahead** configuration file:

  ```
  READAHEAD_COLLECT="no"
  READAHEAD_COLLECT_ON_RPM="no"
  ```

  Alternatively, the **readahead** package can be removed entirely.

- An error exists in the communication process between the samba daemon and the Common Unix Printing System (CUPS) scheduler. Consequently, the first time a print job is submitted to a Red Hat Enterprise Linux 6 system via Server Message Block (SMB), a timeout will occur. To work around this issue, use the following command to create a CUPS certificate before the first print job is submitted:

  ```
  lpstat -E -s
  ```

- Under some circumstances, using the **rhn_register** command to register a system with the Red Hat Network (RHN) might fail. When this issue is encountered, the rhn_register command will return an error similar to:

  ```
  # rhn_register
  Segmentation fault (core dumped)
  or
  # rhn_register
  ***MEMORY-ERROR***: rhn_register[11525]: GSlice: assertion failed:
  sinfo->n_allocated > 0
  Aborted (core dumped)
  ```

To work around this issue, set the following environment variable, then run the rhn_register command again:

```
G_SLICE=always-malloc
```

- If a user has a .bashrc which outputs to stderr, the user will be unable to sftp into their account. From the user's point of view, the sftp session is immediately terminated after authentication.

2.1.1. Architecture Specific Known Issues

2.1.1.1. System z

The minimum hardware requirement to run Red Hat Enterprise Linux Beta is IBM System z9 (or better). The system may not IPL (i.e. boot) on earlier System Z hardware (e.g. z900 or z990)

2.1.1.2. IBM POWER (64-bit)

- When network booting an IBM POWER5 series system, you may encounter an error such as:

  ```
  DEFAULT CATCH!, exception-handler=fff00300
  ```

  If the path that locates the kernel and ramdisk is greater than 63 characters long, it will overflow a firmware buffer and the firmware will drop into the debugger.

  POWER6 and POWER7 firmware includes a correction for this problem. Note that IBM POWER5 series is not a supported system.

- On some machines yaboot may not boot, returning the error message:

  ```
  Cannot load ramdisk.image.gz: Claim failed for initrd memory at 02000000 rc=ffffffff
  ```

  To work around this issue, change real-base from to **c00000**. Real-base can be obtained from OpenFirmware prompt with the **printenv** command and set with **setenv** command.

- Remote installs on IBM BladeCenter JS22 servers may encounter the following error message:

  ```
  No video available. Your server may be in an unsupported resolution/refresh rate.
  ```

  To work around this issue, specify the following GUI parameters:

  ```
  video=SVIDEO-1:d radeon.svideo=0
  ```

- 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".

- filecap crashes with a segmentation fault when run directly on an empty file. For example:

  ```
  # filecap /path/to/empty_file
  Segmentation fault (core dumped)
  ```

To work around this, run filecap on the directory that contains the empty file, and search the results for the required information. For example:

```
filecap /path/to/ | grep empty_file
```

- A change in the package that the sos tool uses to determine the installed version of Red Hat Enterprise Linux will cause the tool to incorrectly identify the major release version. This adversely impacts a small number of non-default sos plugins and may cause incomplete information to be captured from the system when these plugins are enabled. The affected plugins are:
  - general (only when using the non-default all_logs option)
  - cluster (diagnostics may not be run)

  Users affected by this problem should retrieve any missing data manually from systems.

3. VIRTUALIZATION

Para Virtualization on Hardware Virtualized Machines (PV on HVM)

Red Hat Enterprise Linux 6 guests under Red Hat Enterprise Linux 5 Xen hosts can now utilize the PV on HVM drivers to improve the performance of I/O on virtualized network devices (xen-vnif) and virtualized block storage devices.

To enable Xen PV on HVM support in a Red Hat Enterprise Linux 6 HVM guest, add the following to the kernel boot command line:

```
xen_pv_hvm=enable
```

Note, however, that due to conflicts with network configuration scripts, it is recommended that the xen guest vif specification set 'type=netfront' if the emulated rtl8139 device is not desired as the primary network interconnect.

virtio network device packet transmission algorithms

The virtio network device has two available algorithms for transmitting packets. The default is to use an asynchronous bottom half transmitter which typically shows good performance for all workloads. The alternate implementation uses a timer to delay transmit in an attempt to batch multiple packets together. The timer approach typically results higher latency, but may improve overall efficiency. To change from the default algorithm to the timer based approach, use the following procedure to create a wrapper script around qemu-kvm and specify it as the emulator for guests that require it.

1. create the wrapper script

```
$ cat > /usr/libexec/qemu-kvm.txtimer << EOF
#!/bin/sh
exec /usr/libexec/qemu-kvm \`echo "\$@" | sed
's|virtio-net-pci|virtio-net-pci,tx=timer|g'\`
EOF
```

2. Make script executable

```
$ chmod 755 /usr/libexec/qemu-kvm.txtimer
```

3. Set selinux permissions

```
$ restorecon /usr/libexec/qemu-kvm.txtimer
```

4. Create selinux module

```
$ cat > qemutxtimer.te << EOF
policy_module(qemutxtimer, 1.0)

gen_require(\`
 attribute virt_domain;
 type qemu_exec_t;
')

can_exec(virt_domain, qemu_exec_t)
EOF
```

5. Build selinux module

```
$ make -f /usr/share/selinux/devel/Makefile
```

6. Install selinux module

```
$ semodule -i qemutxtimer.pp # May later be uninstalled with -r
```

7. Update guest XML to use qemu-kvm wrapper

```
$ virsh edit $GUEST
```

Replace:

```
    <emulator>/usr/libexec/qemu-kvm</emulator>
```

With:

```
    <emulator>/usr/libexec/qemu-kvm.txtimer</emulator>
```

3.1. Known Issues

- Under some circumstances, installation of a Red Hat Enterprise Linux 6 virtual guest stalls after the optional testing of media. Note that this issue has only been observed with Red Hat Enterprise Linux 6 guests that utilize multiple virtualized CPUs. To work around this issue, use a media source that is known to be verified, and skip the media test, or use a single virtualized CPU during installation.

- Cancelling the disk physical cache for block devices and use of barriers for filesystems may slow down qcow2 dramatically. Use the following command to reduce the frequency of sync requests by pre-allocating new images and setting the cluster size to 2M

```
./qemu-img create  -opreallocation=metadata -ocluster_size=2M -f qcow2 $DISK $SIZE
```

- 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 /etc/libvirt/qemu.conf, set "relaxed_acs_check = 1", and restart libvirtd. Note that this action will re-open possible security issues.

- Users upgrading from pre-release versions of Red Hat Enterprise Linux 6 (i.e. the **virt-v2v** versions less than virt-v2v-0.6.2-2.el6) may be required to update the default virt-v2v configuration file. Specifically, the 'viostor' app for Windows guests is replaced by the 'virtio' app, which now points to the directory containing the complete driver. Refer to the updated default configuration file for further details.

- I/O Advanced Programmable Interrupt Controller (I/O APIC) timer interrupts are not emulated as non-maskable interrupts (NMIs) to virtualized guests. Consequently, if a virtualized guest uses the kernel parameter **nmi_watchdog=1**, the guest kernel will panic on boot.

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

- Direct Asynchronous IO (AIO) that is not issued on filesystem block boundaries, and falls into a hole in a sparse file on ext4 or xfs filesystems, may corrupt file data if multiple I/O operations modify the same filesystem block. Specifically, if qemu-kvm is used with the aio=native IO mode over a sparse device image hosted on the ext4 or xfs filesystem, guest filesystem corruption will occur if partitions are not aligned with the host filesystem block size. Generally, do not use aio=native option along with cache=none for QEMU. This issue can be avoided by using one of the following techniques:

  1. Align AIOs on filesystem block boundaries, or do not write to sparse files using AIO on xfs or ext4 filesystems.

  2. KVM: Use a non-sparse system image file or allocate the space by zeroing out the entire file.

  3. KVM: Create the image using an ext3 host filesystem instead of ext4.

  4. KVM: Invoke qemu-kvm with aio=threads (this is the default).

  5. KVM: Align all partitions within the guest image to the host's filesystem block boundary (default 4k).

- On Red Hat Enterprise Linux 6 KVM virtual guests, unmounting a filesystem on an mdraid volume does not immediately free the underlying device for the **mdadm --stop operation**. Consequently, during installation on a system with pre-existing mdraid volumes the following error can appear while anaconda is looking for storage devices:

  > MDRaidError: mddeactivate failed for /dev/md1: 08:26:59,485 ERROR : Perhaps a running process, mounted filesystem or active volume group?

  To work around this issue, erase all data on the volume before installation by clearing the first several sectors of the volume with zeros.

- Libvirt uses transient iptables rules for managing NAT or bridging to virtual machine guests. Any external command that reloads 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 command 'service libvirt reload' to restore libvirt's additional iptables rules.

- Adding an rtl8139 NIC to an active Windows 2008 guest may result in the qemu-kvm process exiting. To work around this issue, shutdown the guest before adding additional rtl8139 NICs. Alternatively, install the virtio-net drivers and add a virtio NIC.

- KVM users with a mix of virtio and ata disks should verify the boot device that anaconda

chooses during installation. To verify the boot device, locate the "Install Target Devices" list in the disk selection screen that follows the partitioning type screen. Verify the boot device selection, which is indicated by a selector in the left-most column of the "Install Target Devices" list.

- When installing Red Hat Enterprise Linux 6 as a new KVM guest, installer may incorrectly report amount of free memory available. Consequently, installation may terminate or switch to the text user interface. To work around this issue, increase amount of RAM allocated for the guest to 128 MB more than specified for the architecture and installation method.

- 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.

- Under some circumstances, if an 82576 Network driver (igb) is reloaded with the ***max_vfs=8*** parameter and an uncorrectable PCIe AER error is seen on its port, the operation will hang or crash the host system. This error has been encountered with two 82576 devices connected via an IDT PES12N3A PCI Express Switch (rev 0c) plugged into a Westmere-EP's 5520/5500/X58 I/O Hub PCI Express Root Port 3. Note that other 82576 devices and IDT switches have worked in other Westmere-based systems

  If the error occurs, two workarounds have been found to enable the use of all eight virtual functions (VFs) for guest virtual machines(VMs):

  1. Reload the 82576 driver with max_vfs=1, then unload, then reload with max_vfs=8. For example:

     ```
     rmmod igb
     modprobe igb max_vfs=1
     rmmmod igbvf
     rmmod igb
     modprobe igb max_vfs=8
     ```

  2. If PCI AER functionality is not needed in the host, boot the kernel with the parameter setting: ***pci=noaer***

- A dual function, 82576 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 is able to convert guests running on ESX server. A current limitation in virt-v2v means that 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 underlying storage are on different datastores, virt-v2v will report a 404 error while trying to retrieve the storage.

- Under some circumstances, the virtio queue will fill if an application on a guest repeatedly writes to a **virtio-serial** character device while the host is not processing the queue. Consequently, the guest will enter an infinite loop and appear to be hung. Once the host side of the character device is read from, the guest will return to normal functionality.

- The qemu-kvm options to enable VMware device emulation are not functional or supported in Red Hat Enterprise Linux 6.

- Avoid running guestfish (without the --ro option), virt-edit, virt-tar (in upload mode), virt-win-reg (in merge mode) or guestmount (without the --ro option) on live virtual machine disks. If any of these tools are used on live virtual machines, disk corruption might occur.

4. STORAGE AND FILESYSTEMS

The ext4 Filesystem

The ext4 file system is a scalable extension of the ext3 file system, which was the default file system of Red Hat Enterprise Linux 5. Ext4 is now the default file system of Red Hat Enterprise Linux 6

Because of delayed allocation and other performance optimizations, ext4's behavior of writing files to disk is different from ext3. In ext4, a program's writes to the file system are not guaranteed to be on-disk unless the program issues an fsync() call afterwards.

Further information on the allocation features of ext4 is available in the Storage Administration Guide

CIFS servers that require plaintext passwords

Some Common Internet File System (CIFS) servers require plaintext passwords for authentication. Support for plaintext password authentication can be enabled using the command:

```
echo 0x37 > /proc/fs/cifs/SecurityFlags
```

WARNING

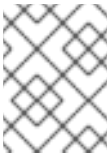
This operation can expose passwords by removing password encryption.

Event Tracing in GFS2

GFS2's event tracing is provided via the generic tracing infrastructure. The events are designed to be useful for debugging purposes. Note, however that it is not guaranteed that the GFS2 events will remain the same throughout the lifetime of Red Hat Enterprise Linux 6. Further details on GFS2's glocks and event tracing can be found in the following 2009 Linus Symposium paper: http://kernel.org/doc/ols/2009/ols2009-pages-311-318.pdf

mpi-selector

The mpi-selector package has been deprecated in Red Hat Enterprise Linux 6. **environment-modules** is now used to select which Message Passing Interface (MPI) implementation is to be used.



NOTE

The man page for the **module** command contains detailed documentation for the **environment-modules** package.

To return a list of what modules are available, use:

```
module avail
```

To load or unload a module use the following commands:

```
module load <module-name>
module unload <module-name>
```

To emulate the behavior of mpi-selector, the module load commands must be place in the shell init script (e.g. /**.bashrc**) to load the modules every login.

4.1. Technology Previews

fsfreeze

Red Hat Enterprise Linux 6 includes **fsfreeze** as a Technology Preview. **fsfreeze** is a new command that halts access to a filesystem on disk. **fsfreeze** is designed to be used with hardware RAID devices, assisting in the creation of volume snapshots. Further details on **fsfreeze** are in 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 filesystem that does not fall back to buffered IO when doing certain allocation operations.) Only applications designed for use with O_DIRECT I/O and DIF/DIX hardware should enable this feature. Red Hat Enterprise Linux 6 includes the Emulex LPFC driver version 8.3.5.17, introducing support for DIF/DIX. For more information, refer to the Storage Administration Guide

Filesystem in Userspace

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

LVM Snapshots of Mirrors

The LVM snapshot feature provides the ability to create backup images of a logical volume at a particular instant without causing a service interruption. When a change is made to the original device (the origin) after a snapshot is taken, the snapshot feature makes a copy of the changed data area as it was prior to the change so that it can reconstruct the state of the device. Red Hat Enterprise Linux 6 introduces the ability to take a snapshot of a mirrored logical volume.

A known issue exists with this Technology Preview. I/O might hang if a device failure in the mirror is encountered. Note, that this issue is related to a failure of the mirror log device, and that no work around is currently known.

btrfs

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 the x86_64 architecture.

WARNING

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

FS-Cache

FS-Cache is a new feature in Red Hat Enterprise Linux 6 Beta 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.

4.2. Known Issues

- Mounting file systems on a guest using the **-o nobarrier** option is not recommended, even if the host is directly conneted to Enterprise-class storage.

- When an LVM mirror suffers a device failure, a two-stage recovery takes place. The first stage involves removing the failed devices. This can result in the mirror being reduced to a linear device. The second stage — if configured to do so by the administrator — is to attempt to replace any of the failed devices. Note, however, that there is no guarantee that the second stage will choose devices previously in-use by the mirror that had not been part of the failure if others are available.

- In Red Hat Enterprise Linux 5, infiniband support (specifically the **openib** start script and the **openib.conf** file) were supplied by the **openib** package. In Red Hat Enterprise Linux 6, the **openib** package is renamed to rdma. Additionally, the service has been renamed to rdma and the configuration file is now located in **/etc/rdma/rdma.conf**.

- 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.

- If a device-mapper-multipath device is still open, but all of the attached paths have been lost, the device is unable to create a new table with no paths. Consequently, the following unusual output may be returned from the **multipath -ll output** command:

```
mpatha (3600a59a0000c2fd0003079284c122fec) dm-0,
size=2.0G hwhandler='0'
|-+- policy='round-robin 0' prio=0 status=enabled
```

```
| `- #:#:#:# -   #:#  failed faulty running
`-+- policy='round-robin 0' prio=0 status=enabled
  |- #:#:#:# -   #:#  failed faulty running
  `- #:#:#:# -   #:#  failed faulty running
```

Output of this type indicates that there are no paths to the device. The erroneous lines in the output preceded by the string **#:#:#:#** will be removed in a future release.

- **ext2** and **ext3** filesystems do not use a **page_mkwrite** mechanism to intercept page faults. The quota subsystem can not account for this additional usage when writing to disk. Consequently, a user may exceed their disk block quota by issuing memory-mapped writes into a sparse region of a file. Note, also, that this is a longstanding behavior in the ext2 and ext3 filesystems.

- **Parted** in Red Hat Enterprise Linux 6 cannot handle Extended Address Volumes (EAV) Direct Access Storage Devices (DASD) that have greater 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 installation using the tools provided in **s390-utils**.

- Systems that have an Emulex FC controller (with SLI-3 based firmware) installed may return a kernel panic during install. If the SAN disk is not required for installation, work around this issue by disconnecting the SAN connection from the Emulex FC controller. Note that this issue does not occur on SLI-4 based controllers. To determine the firmware interface of the adapter, run the command

  ```
  cat /sys/class/scsi_host/host{n}/fwrev
  ```

- When multipath is configured to use user_friendly_names, it stores the binding between the wwid and the alias in /etc/multipath/bindings. When multipath creates devices in early bootup, (for example when the root filesystem is on a multipath device) it looks at /etc/multipath/bindings in the initramfs. When it creates devices during normal operation, it looks at /etc/multipath/bindings in the root filesystem. Currently, these two files aren't synced during initramfs creation. Because of this, there may be naming conflicts which keep new multipath devices from being created after bootup. To work around this, the bindings for the devices created by the initramfs must be copied into /etc/multipath/bindings after installation. The format of the bindings is:

  ```
  <alias><space><wwid>
  ```

  for example:

  ```
  mpatha 3600d0230000000000e13955cc3757801
  ```

- Direct Asynchronous IO (AIO) that is not issued on filesystem block boundaries, and falls into a hole in a sparse file on ext4 or xfs filesystems, may corrupt file data if multiple I/O operations modify the same filesystem block. Specifically, if qemu-kvm is used with the aio=native IO mode over a sparse device image hosted on the ext4 or xfs filesystem, guest filesystem corruption will occur if partitions are not aligned with the host filesystem block size. Generally, do not use aio=native option along with cache=none for QEMU. This issue can be avoided by using one of the following techniques:

  1. Align AIOs on filesystem block boundaries, or do not write to sparse files using AIO on xfs or ext4 filesystems.

  2. KVM: Use a non-sparse system image file or allocate the space by zeroing out the entire file.

3. KVM: Create the image using an ext3 host filesystem instead of ext4.

4. KVM: Invoke qemu-kvm with aio=threads (this is the default).

5. KVM: Align all partitions within the guest image to the host's filesystem block boundary (default 4k).

- Mixing the iSCSI **discoveryd** mode and the normal discovery mode is not supported. When using **discoveryd** mode, **iscsid** will attempt to login from all iSCSI **ifaces** found in **/var/lib/iscsi/ifaces**. If the **iface** cannot log into the target this will fill the log with failure messages every **discoveryd_poll_inval** seconds. To prevent this, the **iface** can be deleted by running "**iscsiadm -m iface -o delete -I ifacename**".

- A change in the 2.6.31 Linux kernel made the ***net.ipv4.conf.default.rp_filter = 1*** more strict in the I/O that is accepted. Consequently, in Red Hat Enterprise Linux 6, if there are multiple interfaces on the same subnet and I/O is sent to the one that is not the default route, the I/O will be dropped. Note that this applies to iSCSI iface binding when multiple interfaces are on the same subnet. To work around this, set the ***net.ipv4.conf.default.rp_filter*** parameter in **/etc/sysctl.conf** to 0 or 2, and reboot the machine.

- Attempting to run multiple LVM commands in quick succession might cause a backlog of these commands. Consequently, some of the operations requested might time-out, and subsequently, fail.

- dracut 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 (e.g. using RAID, LVM or similar techniques) is not possible.

- If an LVM volume requires physical volumes that are multipath or FCoE devices, the LVM volume will not automatically activate. To enable automatic LVM activation, create a udev rules file /etc/udev/rules.d/64-autolvm.rules with the following content:

```
SUBSYSTEM!="block", GOTO="lvm_end"
ACTION!="add|change", GOTO="lvm_end"
KERNEL=="dm-[0-9]*", ACTION=="add", GOTO="lvm_end"
ENV{ID_FS_TYPE}!="LVM*_member", GOTO="lvm_end"

PROGRAM=="/bin/sh -c 'for i in $sys/$devpath/holders/dm-[0-9]*; do [ -e $$i ] && exit 0;
done; exit 1;' ", \
    GOTO="lvm_end"

RUN+="/bin/sh -c '/sbin/lvm vgscan; /sbin/lvm vgchange -a y'"

LABEL="lvm_end"
```

  Note, however that this work around may impact system performance.

- The fscontext=, defcontext=, rootcontext= or context= mount options should not be used for remount operations. Using these options can cause the remount of a manually mounted volume to fail, returning errors such as:

```
mount: /dev/shm not mounted already, or bad option
```

5. NETWORKING

NetworkManager

NetworkManager is enabled by default if it is installed. However, **NetworkManager** is only installed by default in the client use cases. **NetworkManager** is available to be installed for the server use cases, but is not included in the default installation.

5.1. Technology Previews

IPv6 support in IPVS

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

5.2. Known Issues

- If the **qeth** interface was previously configured using system-config-network **1.6.0.el6.2**, the "OPTIONS=" line needs to be manually added to **/etc/sysconfig/network-scripts/ifcfg-<interface>**.

  After the configuration has been manually changed, activate the interface by either rebooting the system, or running the following commands:

  ```
  # /sbin/znet_cio_free
  # SUBSYSTEM="ccw" DEVPATH="bus/ccw/devices/<SUBCHANNEL 0>" /lib/udev/ccw_init
  # ifup <interface>
  ```

- A known issue in the bnx2 driver prevents BCM5709S network adapters from performing a vmcore core dump over NFS.

- Intel 82575EB ethernet devices do not function in a 32 bit environment. To work around this issue, modify the kernel parameters to include the **intel_iommu=off** option.

- Running the **rds-ping** command may fail, returning the error:

  ```
  bind() failed, errno: 99 (Cannot assign requested address).
  ```

  Note, also that this error may occur even with ***LOAD_RDS=yes*** set in **/etc/rdma/rdma.conf**. To work around this issue, load the **rds-tcp** module.

- Running the command **rds-stress** on a client may result in the following error attempting to connect to the server:

  ```
  connecting to <server IP address>:4000: No route to host
  connect(<server IP address>) failed#
  ```

- When configuring a network interface manually, including static IP addresses and search domains, it is possible that a **search** entry will not be propagated to **/etc/resolv.conf**. Consequently, short host names that do not include the domain name will fail to resolve. To workaround this issue, add a **search** entry manually to **/etc/resolv.conf**.

- Under some circumstances, the NetworkManager panel applet cannot determine if a user has permission to enable networking. Consequently, after logging into the desktop, the "Enable Networking" and "Enable Wireless" checkboxes may be disabled. To work around this, run the following command as root:

```
touch /usr/share/polkit-1/actions/org.freedesktop.NetworkManager.policy
```

Alternatively, WiFi can be enabled using the command:

```
nmcli nm wifi on
```

or disabled using the command:

```
nmcli nm wifi off
```

- Under some circumstances, the **netcf** command crashes, returning the error message:

```
Failed to initialize netcf
error: unspecified error
```

To work around this issue, set the following value in /etc/sysctl.conf:

```
net.bridge.bridge-nf-call-iptables = 0
```

This issue presents when the **augeas** library (used by **netcf**) has trouble parsing one of the system config files that netcf needs to read or modify.

- The default value of the Emulex lpfc module parameter, lpfc_use_msi, was 2 (MSI-X) on Red Hat Enterprise Linux 5.4. In Red Hat Enterprise Linux 6 this default is now set to 0 (INTx). This change causes the driver behavior to stop using MSI-X interrupt mode and reverts to using non-msi (INTx) interrupt mode. This change in defaults addresses apparent regressions in some hardware platforms, introduced when the default lpfc driver value was previously changed from 0 to 2 (which made MSI-X the default behavior).

  If the lpfc module is behaving erratically, work around this issue by setting the lpfc module parameter lpfc_use_msi to 2.

6. CLUSTERING

6.1. Technology Previews

pacemaker

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.

6.2. Known Issues

- Supplying an invalid version number in cluster.conf as a parameter to the cman_tool command will cause the cluster to stop processing information. To work around this issue, ensure that the version number used is valid.

- Under some circumstances, creating cluster mirrors with the '--nosync' option may cause I/O to become extremely slow. Note that this issue only effects I/O immediately after the creation of the mirror, and only when '--nosync' is used. To work around this issue, run the following command after the creating the mirror.

```
lvchange --refresh <VG>/<LV>
```

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

- The sync state of an inactive LVM mirror cannot be determined. Consequently, the primary device of an LVM mirror can only be removed when the mirror is in-sync.

- If device-mapper-multipath is used, and the default path failure timeout value (**/sys/class/fc_remote_ports/rport-xxx/dev_loss_tmo**) is changed, that the timeout value will revert to the default value after a path fails, and later restored. Note that this issue will present the lpfc, qla2xxx, ibmfc or fnic Fibre Channel drivers. To work around this issue the dev_loss_tmo value must be adjusted after each path fail/restore event.

- Generally, placing mirror legs on different physical devices improves data availability. The command **lvcreate --alloc anywhere** does not guarantee placement of data on different physical devices. Consequently, the use of this option is not recommended. If this option is used, the location of the data placement must be manually verified.

- The GFS2 fsck program, fsck.gfs2, currently assumes that the gfs2 file system is divided into evenly-spaced segments known as resource groups. This is always the case on file systems formatted by mkfs.gfs2. It will also be the case for most file systems created as GFS (gfs1) and converted to gfs2 format with gfs2_convert. However, if a GFS file system was resized (with gfs_grow) while it was in the GFS format, the resource groups might not be evenly spaced. If the resource groups are not evenly spaced, and the resource groups or the resource groups index (rindex) become damaged, fsck.gfs2 might not function correctly.

  There is currently no workaround for this issue. However, if the resource groups are not damaged, avoid this issue by copying the file system contents to a new device with evenly-spaced resource groups. Format the new device as gfs2 with mkfs.gfs2, and copy the contents from the old device to the new device. The new device will have evenly-spaced resource groups.

7. AUTHENTICATION

7.1. Technology Previews

certmonger

The certmonger service aims to manage certificates on behalf of services running on client systems. It warns administrators when a certificate which it has been asked to watch is nearing the end of its validity period, and can be told to attempt to automatically obtain a new certificate when this happens. It supports certificates and private keys stored in either PEM or NSS database formats. It can interact with CAs running either IPA or certmaster, and is intended to be extensible to support other implementations.

ipa-client

IPA is an integrated solution to provide centrally managed Identity (machine,user, virtual machines, groups, authentication credentials). This package includes client-side functionality that when combined with a supported server can be used to provide features like kerberized sshd.

7.2. Known Issues

- Enabling user authentication against an LDAP server using **authconfig --enableldapauth** does not correctly set up the **/etc/nslcd.conf** configuration file. Consequently, LDAP users will be denied access to the system. To work around this issue, remove the line containing

pam_password md5 from the **/etc/nslcd.conf** file.

- The System Security Services Daemon (SSSD) currently supports following LDAP referrals on anonymous-bind LDAP connections only.
- The authentication configuration utility does not keep the 'Require smart card for login' check box set when Kerberos is also enabled. When the check box is checked and the configuration is saved with the 'Apply' button, the system will correctly require smart card for login. However, on the subsequent run of the authentication configuration utility the check box will be unchecked again and it is necessary to check it again to keep the option switched on.
- When attempting to perform PKINIT pre-authentication, if the client has more than one possible candidate certificate the client may fail to select the certificate and key to use. This usually occurs if certificate selection is configured to use the value of the keyUsage extension, or if any of the candidate certificates does not contain a **subjectAltName** extension. Consequently, the client attempts to perform pre-authentication using a different (usually password-based) mechanism.
- After installing certmonger, the system message bus daemon needs to be signaled to reload its configuration to allow the certmonger service to start properly. To work around this issue, send the dbus-daemon process a SIGHUP signal, or, alternatively, reboot the system.

8. SECURITY

8.1. Technology Previews

OpenSCAP

OpenSCAP is a set of open source libraries that support the Security Content Automation Protocol (SCAP) standards from the National Institute of Standards and Technology (NIST). OpenSCAP supports the SCAP components:

- Common Vulnerabilities and Exposures (CVE)
- Common Platform Enumeration (CPE)
- Common Configuration Enumeration (CCE)
- Common Vulnerability Scoring System (CVSS)
- Open Vulnerability and Assessment Language (OVAL)
- Extensible Configuration Checklist Description Format (XCCDF)

Additionally, the openSCAP package includes an application to generate SCAP reports about system configuration. This package is considered a Technology Preview in Red Hat Enterprise Linux 6.

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 in this Red Hat Enterprise Linux 6.

9. DEVICES AND DEVICE DRIVERS

PCI Device Ordering

In Red Hat Enterprise Linux 6, the PCI device ordering is based on the PCI device enumeration. PCI device enumeration is based on the PCI enumeration algorithm (depth first then breadth) and is constant per system type. Additionally, once the devices are discovered, the module loading process is sequentialized, providing persistent naming of the interfaces.

9.1. Technology Previews

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

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

9.2. Known Issues

- The **udev** daemon in Red Hat Enterprise 6 watches all devices for changes. If a change occurs, the device is rescanned for device information to be stored in the udev database.

  The scanning process causes additional I/O to devices after they were changed by tools. udev to can be told to exclude devices from being watched with a udev rule. A rule can be created by adding a new file **<myname>.rules** in **/etc/udev/rules.d** containing the following line:

  ```
  ACTION=="add|change", SYMLINK=="disk/by-id/scsi-
  SATA_SAMSUNG_HD400LDS0AXJ1LL903246", OPTIONS+="nowatch"
  ```

  The SYMLINK should be replaced with any symlink path found in /dev/disk/* for the device in question.

  This will prevent unexpected I/O on the device, after data was written directly to the device (not on the filesystem). However, it will also prevent device updates in the udev database, like filesystem labels, symbolic links in /dev/disk/*, etc.

- Under some circumstances, the **bfa-firmware** package in Red Hat Enterprise Linux 6 may cause these devices to encounter a rare memory parity error. To work around this issue, to update to the newer firmware package, available directly from Brocade.

- 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 command

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

  will return the version of the device being used in an individual machine.

- 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.

- Partial Offload iSCSI adapters do not work on Red Hat Enterprise Linux. Consequently, devices that use the be2iscsi driver cannot be used during installation.

- The **hpsa_allow_any** kernel option allows the **hpsa** driver to be used with older hardware that typically uses the **cciss** module by default. To use the **hpsa** driver with older hardware, set **hpsa_allow_any=1** and blacklist the **cciss** module. Note, however that this is an unsupported, non-default configuration.

- Platforms with BIOS/UEFI that are unaware of PCI-e SR-IOV capabilities may fail to enable virtual functions

- The recommended minimum HBA firmware revision for use with the mpt2sas driver is "Phase 5 firmware" (i.e. 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.

- The persistent naming of devices that are dynamically discovered in a system is a large problem that exists both in and outside of kdump. Nominally, 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 (e.g. LVM) make essentially resolve the issue, though 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.

- The following issues and limitations may be encountered with the Broadcom **bnx2**, **bnx2x**, and **cnic** drivers

    - Support for only one VLAN per port

    - If deactivating the interface (i.e. the **ifdown** and **ifup** commands) the driver will need to be unloaded and reloaded to function correctly.

10. KERNEL

Kdump Auto Enablement

Kdump is now enabled by default on systems with large amounts of memory. Specifically, kdump is enabled by default on:

- systems with more than 4GB of memory on architectures with a 4KB page size (i.e. x86 or x86_64), or

- systems with more than 8GB of memory on architectures with larger than a 4KB page size (i.e PPC64).

On systems with less than the above memory configurations, kdump is not auto enabled. Refer to **/usr/share/doc/kexec-tools-2.0.0/kexec-kdump-howto.txt** for instructions on enabling kdump on these systems.

crashkernel parameter syntax

Please note that in future versions of Red Hat Enterprise Linux 6 (i.e. Red Hat Enterprise Linux 6.1 and later) the **auto** value setting of the **crashkernel=** parameter (i.e. **crashkernel=auto**) will be deprecated.

Barrier Implementation in the Kernel

The barrier implementation in the Red Hat Enterprise Linux 6 kernel works by completely draining the I/O scheduler's queue, then issuing a preflush, a barrier, and finally a postflush request. However, since the supported file systems in Red Hat Enterprise Linux 6 all implement their own ordering guarantees, the block layer need only provide a mechanism to ensure that a barrier request is ordered with respect to other I/O already in the disk cache. This mechanism avoids I/O stalls experienced by queue draining. The block layer will be updated in future kernels to provide this more efficient mechanism of ensuring ordering.

Workloads that include heavy fsync or metadata activity will see an overall improvement in disk performance. Users taking advantage of the proportional weight I/O controller will also see a boost in performance. In preparation for the block layer updates, third party file system developers need to ensure that data ordering surrounding journal commits are handled within the file system itself, since the block layer will no longer provide this functionality.

These future block layer improvements will change some kernel interfaces such that symbols which are not on the kABI whitelist shall be modified. This may result in the need to recompile third party file system or storage drivers.

Systemtap Tracepoints

The following 3 virtual memory tracepoints are deprecated in Red Hat Enterprise Linux 6

- trace_mm_background_writeout(unsigned long written)
- trace_mm_olddata_writeout(unsigned long written)
- trace_mm_balancedirty_writeout(unsigned long written)

10.1. Technology Previews

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 (NameSpace) Containers [LXC] is a Technology Preview feature in Red Hat Enterprise Linux 6 Beta that provides isolation of resources assigned to one or more processes. A process is assigned a separate user permission, networking, filesystem name space from its parent.

10.2. Known Issues

- Calgary IOMMU default detection has been disabled in this release. If you require Calgary IOMMU support add 'iommu=calgary' as a boot parameter.

- The kdump service fails on systems with large amounts of memory and **crashkernel=auto** enabled, returning the error message **kdump: kexec: failed to load kdump kernel** in **/var/log/messages**.

  To workaround this issue, change the **crashkernel** parameter to **128M** (on x86_64 and x86 architectures) or **256M** (on the ppc64 architecture).

- If the kdump crash recovery technology is enabled and in use on a given system, minimum memory requirements should be raised by the amount of memory reserved for kdump usage. This value is determined by the user, and specified on the kernel command line, via the crashkernel parameter. The default value for this setting is 128MB.

- When using the DIF/DIX hardware checksum features of a storage path behind a block device, errors will occur if the block device is used as a general purpose block device.

  Buffered I/O or mmap(2) based IO will not work reliably as there are no interlocks in the buffered write path to prevent overwriting cached data while the hardware is performing DMA operations. An overwrite during a DMA operation will cause a torn write and the write will fail checksums in the hardware storage path. This problem is common to all block device or file system based buffered or mmap(2) I/O, so the problem of I/O errors during overwrites cannot be worked around.

  DIF/DIX enabled block devices should only be used with applications that use O_DIRECT I/O. Applications should use the raw block device, though it should be safe to use the XFS file system on a DIF/DIX enabled block device if only O_DIRECT I/O is issued through the file system. In both cases the responsibility for preventing torn writes lies with the application, so only applications designed for use with O_DIRECT I/O and DIF/DIX hardware should enable this feature.

- The memory controller in Red Hat Enterprise Linux 6 beta may encounter stability issues when under heavy stress testing or memory pressure.

- The i686 debug kernel may crash on some systems when starting the udev service.

- Systems configured with Intel 82578DM NICs may not be recognized during boot/install resulting in driver load failure, (driver probe fails with error -2).

- This pre-release version of Red Hat Enterprise Linux 6 provides automated Physical CPU Socket and Memory Hot-Add support. Note, however, that CPU Socket and Memory Hot-Remove actions are not supported. Additionally, only single CPU Socket add events are supported at this time, and tsc support is disabled after a CPU Socket add event.

- In Beta releases of Red Hat Enterprise Linux 6, PCIe ASPM would be enabled on PCIe hierarchies even if they lacked an _OSC method as defined in section 4.5 of the PCI firmware specification, release 3.0. Post Beta, firmware must provide an appropriate _OSC method on all PCI roots in order to allow PCIe ASPM to be enabled. The "pcie_aspm=force" boot parameter may be passed in order to enable PCIe ASPM.

- Use of the cciss and hpsa drivers with some controllers (e.g. P400, P400i, E500, P800, P700m and 6402/6404) may cause kdump to fail.

- The top-level makefile to of the kernel in Red Hat Enterprise Linux 6 includes the -Werror option as part of the standard kernel build. Consequently, all kernel compile warnings are reported as errors. In non-production environments, the -Werror flag can be disabled by removing the following two lines from the top-level kernel Makefile:

```
KBUILD_CFLAGS   += $(shell if [ $(CPP_VERS) -ge 4004004 ]; then \
                echo "-Wno-array-bounds -Werror"; else echo ""; fi)
```

Note, however, that Red Hat does not support custom built kernels or custom built modules.

- Some SystemTap probes require the additional module, **uprobes.ko** at run time. This additional module is usually built automatically when the script is compiled. However, in the client-server case, the uprobes.ko module is not returned by the server to the client. Consequently, missing symbols are reported when the module representing the script is loaded. To work around this issue, use the following command to manually build the uprobes.ko module on the client host.

```
make -C <prefix>/share/systemtap/runtime/uprobes
```

Note that "<prefix>" is the install prefix for systemtap, and that this manual build of uprobes.ko will only need to be done once.

- Due to the way ftrace works when modifying the code during startup, 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 using the command:

```
nmi_watchdog=0
```

- Under some circumstances, a kernel panic on installation or boot may occur if the "Interrupt Remapping" feature is enabled in the BIOS. To work around this issue, disable interrupt remapping in the BIOS.

- The kernel will panic when booting the kdump kernel on a s390 system with an initramfs that contains an odd number of bytes. To work around this this issue, generate an initramfs with sufficient padding such that it contains an even number of bytes.

- Creating many 'cpu' control groups (cgroups) on a system with a large number of CPUs will slow down the machine when the control groups feature is enabled. To work around this issue, disable control groups.

- Under certain circumstances, the Linux kernel makes an erroneous assumption about where to reserve memory for the kdump kernel on large-memory POWER systems. Consequently, a newly installed POWER system may return the following message during the initial post installation bootup:

```
returning from prom_init
 Kernel panic - not syncing: ERROR: Failed to allocate 0x4000 bytes below 0x10000000.
 Rebooting in 180 seconds..
```

Complete the following steps to work around this issue. Note, however, that this work around disables the kdump feature.

1. The system will reboot 180 seconds after the initial error message was returned. After reboot, the yaboot prompt will be presented:

```
Welcome to Red Hat Enterprise Linux!
Hit <TAB> for boot options
Welcome to yaboot version 1.3.14 (Red Hat 1.3.14-34.el6)
```

```
Enter "help" to get some basic usage information
boot:
```

At the prompt, enter the following line and press enter.

```
linux crashkernel=512M-2G:256M
```

2. Log in to the system as root, and open /etc/yaboot.conf in a text editor. The yaboot.conf file should be similar to:

```
# yaboot.conf generated by anaconda

boot=/dev/sda1
init-message="Welcome to Red Hat Enterprise Linux!\nHit <TAB> for boot options"

partition=2
timeout=5
install=/usr/lib/yaboot/yaboot
delay=30
enablecdboot
enableofboot
enablenetboot
nonvram
fstype=raw

image=/vmlinuz-2.6.32-59.el6.ppc64
        label=linux
        read-only
        initrd=/initramfs-2.6.32-59.el6.ppc64.img
        append="rd_NO_LUKS rd_NO_LVM rd_NO_MD rd_NO_DM LANG=en_US.UTF-8
SYSFONT=latarcyrheb-sun16 KEYTABLE=us console=hvc0 crashkernel=auto rhgb
quiet root=UUID=63f94acf-6241-4a66-a861-9de912602287"
```

Remove the string **crashkernel=auto** from the **append=** line. Save the file, and exit the editor. Subsequent reboots of the system will boot to the system prompt.

- 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 filesystem, or dumping over SSH.

- 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.

- 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.

- The module loading operation of certain crypto libraries will not be successful. Consequently, the modules required for *in-kernel crypto* cannot be loaded. **In-kernel crypto** cannot be used with Red Hat Enterprise Linux 6 until this issue is resolved.

- A BIOS issue on some platforms incorrectly indicates that the system busmastering flag must be checked before entering the deep C state. Consequently, some systems might spend a significantly lower percentage of time in deep C states (C3 and lower) in Red Hat Enterprise Linux 6 compared to Red Hat Enterprise Linux 5.5. Updated the BIOS on affected systems will resolve this issue.

- IMA in Red Hat Enterprise Linux 6.0 GA is enabled by loading an IMA policy. However, future updates will require the boot parameter "ima=on" in addition to loading an IMA policy to enable IMA. This change reduces overhead on systems not using IMA.

11. DEVELOPMENT AND TOOLS

11.1. Technology Previews

libdfp

An updated libdfp library is available in Red Hat Enterprise Linux 6. libdfp is a decimal floating point math library, and is available as an alternative to the glibc math functions on Power and s390x architectures, and is available in the supplementary channels.

Eclipse Plugins

The following plugins for the Eclipse software development environment are considered to be Technology Previews in this pre-release version of Red Hat Enterprise Linux 6

- The Mylyn plugin for the Eclipse task management subsystem
- the **eclipse-callgraph** C/C++ Call Graph Visualization plugin

11.2. Known Issues

- cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. The cURL API, and consequently, the python bindings for cURL, do not provide textual messages for errors. Therefore, all applications that use the python bindings for cURL will return errors in formats such as:

  ```
  Pycurl Error 6 - ""
  ```

  instead of more useful messages such as:

  ```
  Pycurl Error 6 - "Could not resolve hostname: blah.example.com"
  ```

  cURL error codes can be manually interpreted by reading the **/usr/include/curl/curl.h** file.

- Due to a deficiency in java-1.6.0-ibm-plugin for AMD64 and Intel 64, IBM Java 6 Web Start cannot open JNLP files. This affects file management tools and WWW browsers. To work around this open JNLP files using the command:

  ```
  /usr/lib/jvm/jre-1.6.0-ibm.x86_64/bin/javaws file.jnpl
  ```

  Note that 32-bit packages are not affected by this issue.

- Under some circumstances on the PPC64 architecture, Ruby does not save the context correctly when switching threads. Consequently, when a thread is restored it has a stale value which might return a architecture fault.

- Under some circumstances, libdfp encounters an issue converting some values from string to DFP with the conversion command strtod32. The strtod64 and strtod128 commands do work correctly.

12. DESKTOP

nautilus-open-terminal behavior change

The **nautilus-open-terminal** package provides a right-click "Open Terminal" option to open a new terminal window in the current directory. Previously, when this option was chosen from the Desktop, the new terminal window location defaulted to the user's home directory. However, in Red Hat Enterprise Linux 6, the default behavior opens the Desktop directory (i.e. ~/**Desktop**/). To enable the previous behavior, use the following command to set the **desktop_opens_home_dir** GConf boolean to true:

```
gconftool-2 -s /apps/nautilus-open-terminal/desktop_opens_home_dir --type=bool true
```

Adobe Flash and Adobe Acrobat Reader on 64-Bit

The 64-bit Red Hat Enterprise Linux Supplementary CD contains the 32-bit versions of Adobe Acrobat Reader and Adobe Flash for use on the 64-bit architecture. To use these browser plugins correctly, the **nspluginwrapper.i686** and **alsa-plugins-pulseaudio.i686** packages must be installed prior to the installation of the plugins.

gnome-packagekit architecture filter

By default, gnome-packagekit uses a filter to hide packages that are not the same architecture as the system. Consequently, when installing packages for other architectures (e.g. the 32-bit versions of acroread and flash-plugin on the 64-bit architecture) the "Only native filters" from the Filters menu must be unchecked for these packages to be visible.

12.1. Known Issues

- 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.

- ATI RN50/ES1000 graphics devices have limited Video RAM (VRAM) and are restricted to an 8-bit color depth for the text console. Consequently, the graphical boot screen is unavailable on systems using these graphics devices.

- On the GNOME desktop, the CD/DVD burning utility brasero conflicts with the automounting feature in Nautilus. Consequently, the following error message will be displayed when brasero attempts to verify the checksum of the disc:

  ```
  Error while burning: You do not have the required permissions to use this drive
  ```

  In most cases, the data is still written to the disc.

- The **system-config-users** tool cannot always detect if a home directory can be created correctly. Consequently, system-config-users might fail silently when attempting to create a home directory on some file systems (e.g. home directories located beneath an autofs mount-point). Typically, when this issue is encountered, the user account itself is created, but the creation of the home directory fails. To create a user with an auto-mounted home directory, create the home directory manually before creating the user in system-config-users.

- 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 (i.e. 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.

- Not all languages have predefined default input method engines. Consequently, in some languages, **ibus** will not have an input method engine configured. To work around this issue, add an input method using the Input Method configuration dialog (**System > Preferences > Input Method**

- Using the im-chooser tool, XIM cannot be disabled as the default GTK immodule. Disabling input-methods using im-chooser and restarting the desktop session will still result in GTK applications using the XIM immodule. Consequently, using the Ctrl+Shift+U key combination to the directly input of Unicode characters from their hexidecimal code will not work. To work around this issue, use im-chooser to enable ibus. Enabling ibus permits gtk-im-context-simple's Unicode input and compose sequences to be used.

- The hardware mute button on Lenovo ThinkPad X200 notebooks does not work. Note, however, that the volume down and volume up buttons function correctly.

- The clock applet in the GNOME panel has a default location of Boston, USA. Additional locations are added by 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.

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

- ATI RN50/ES1000 graphics devices have a lower number of hardware controllers than output connectors. Due to a defect in the graphical boot system, this type of configuration results in a blank display. Consequently, users of systems with these ATI graphics devices will experience prolonged (potentially up to 2 minutes or longer) blank screens during boot up and shutdown. Once the boot process completes and a login prompt is available, the display will function as expected. The prolonged blank screen can be avoided by removing "rhgb" from the list of boot parameters on the kernel command line in **/etc/grub.conf**

- If a Russian keyboard is chosen during system installation, the login screen is configured to use Russian input for user names and passwords by default. However, pressing Left Shift and Right Shift does not cause the input to change to ASCII mode. Consequently, the user cannot log in. To work around this issue, run the following sequence, as root, post installation:

  ```
  . /etc/sysconfig/keyboard; echo $LAYOUT | grep -q ",us" && gconftool-2
  --direct --config-source xml:readwrite:/var/lib/gdm/.gconf --set
  /apps/gdm/simple-greeter/recent-layouts --type list --list-type string $(echo
  $LAYOUT | awk -F, '{ print "[" $2 "," $1 "]"; }') && echo "DONE"
  ```

- For KMS drivers, the syntax is:

  ```
  video=[connector:]mode
  ```

  "connector", which is optional maps to the name of the connector as listed in /sys/class/drm/card0. For example:

  ```
  ~% ls /sys/class/drm/card0
  card0-LVDS-1  card0-VGA-1  dev  device  power  subsystem  uevent
  ```

–

This device has connectors named LVDS-1 and VGA-1. If no connector is specified the requested mode will apply to all connectors.

Mode strings may be of the form:

```
<xres>x<yres>[R][-<bpp>][@<refresh>][i][eDd]
```

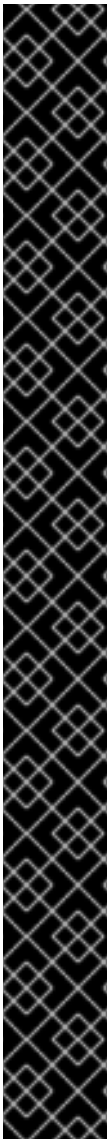
Parts inside <> are mandatory, parts inside [] are optional. R requests the use of the CVT reduced-blanking formula, applicable for some digital displays; otherwise GTF is used. i requests an interlaced mode. e forces the output to be enabled even if it appears to be disconnected; d forces the output to be disabled. For DVI connections, D forces the use of the digital signal path instead of analog; on other connectors it has no effect. Only one of e, d, or D may be given.

- Under some circumstances, the Add/Remove Software (gpk-application) graphical user interface does not display Supplementary groups or packages the Supplementary group is chosen. To work around this, use the System>Refresh Package Lists option to refresh the package lists.

A. PACKAGE MANIFEST

Previous versions of the Technical Notes contained a Package Manifest appendix. The Package Manifest is now available as a seperate document.

B. 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.

B.1. apr

B.1.1. RHSA-2011:0507 – Moderate: apr security update

Updated apr 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 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 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.

CVE-2011-0419

It was discovered that the apr_fnmatch() function used an unconstrained recursion when processing patterns with the '*' wildcard. An attacker could use this flaw to cause an application using this function, which also accepted untrusted input as a pattern for matching (such as an httpd server using the mod_autoindex module), to exhaust all stack memory or use an excessive amount of CPU time when performing matching.

Red Hat would like to thank Maksymilian Arciemowicz for reporting this issue.

All apr users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the apr library, such as httpd, must be restarted for this update to take effect.

B.2. apr-util

B.2.1. RHSA-2010:0950 — Moderate: apr-util security update

Updated apr-util 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 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 Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. apr-util is a library which provides additional utility interfaces for APR; including support for XML parsing, LDAP, database interfaces, URI parsing, and more.

CVE-2010-1623

It was found that certain input could cause the apr-util library to allocate more memory than intended in the apr_brigade_split_line() function. An attacker able to provide input in small chunks to an application using the apr-util library (such as httpd) could possibly use this flaw to trigger high memory consumption.

All apr-util users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the apr-util library, such as httpd, must be restarted for this update to take effect.

B.3. autofs

B.3.1. RHBA-2011:0403 — 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#689754

Prior to this update, an attempt to restart the autofs service while a mounted file system was in use caused the service to stop responding upon its startup. This was due to inappropriate locking during the recursive reconstruction of mount trees of pre-existing mounted multi-mount map entries. With this update, the underlying source code has been adapted to avoid the deadlock during the mount tree reconstruction, so that autofs now starts as expected. Additionally, this update prevents autofs from occasionally terminating with a segmentation fault upon a map entry lookup.

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

B.4. bind

B.4.1. RHSA-2010:0975 – Important: bind security update

Updated bind 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 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.

CVE-2010-3613

It was discovered that named did not invalidate previously cached RRSIG records when adding an NCACHE record for the same entry to the cache. A remote attacker allowed to send recursive DNS queries to named could use this flaw to crash named.

CVE-2010-3614

It was discovered that, in certain cases, named did not properly perform DNSSEC validation of an NS RRset for zones in the middle of a DNSKEY algorithm rollover. This flaw could cause the validator to incorrectly determine that the zone is insecure and not protected by DNSSEC.

All BIND users are advised to upgrade to these updated packages, which contain a backported patch to resolve these issues. After installing the update, the BIND daemon (named) will be restarted automatically.

B.5. bzip2

B.5.1. RHSA-2010:0858 – Important: bzip2 security update

Updated bzip2 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.

bzip2 is a freely available, high-quality data compressor. It provides both standalone compression and decompression utilities, as well as a shared library for use with other programs.

CVE-2010-0405

An integer overflow flaw was discovered in the bzip2 decompression routine. This issue could, when decompressing malformed archives, cause bzip2, or an application linked against the libbz2 library, to crash or, potentially, execute arbitrary code.

Users of bzip2 should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running applications using the libbz2 library must be restarted for the update to take effect.

B.6. chkconfig

B.6.1. RHBA-2012:0417 – chkconfig bug fix update

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

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

Bug Fixes

BZ#797840

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#797839

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.

B.7. cifs-utils

B.7.1. RHBA-2011:0380 – cifs-utils bug fix update

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

The Server Message Block (SMB), also known as Common Internet File System (CIFS), is a standard file-sharing protocol widely deployed on Windows machines. The tools included in this package work in conjunction with support in the kernel to allow users to mount a SMB/CIFS share onto a client, and use it as if it were a standard Linux file system.

Bug Fix

BZ#668366

Due to an error in the cifs.upcall utility, Generic Security Services Application Program Interface (GSSAPI) channel bindings in Kerberos authentication messages were not set properly. This would cause some servers to reject authentication requests. Consequent to this, an attempt to mount a CIFS share with the security mode set to "krb5" could fail with the following error:

```
mount error(5): Input/output error
```

This update corrects the cifs.upcall utility to set the GSSAPI channel bindings properly, and such CIFS shares can now be mounted as expected.

All users of cifs-utils are advised to upgrade to this updated package, which resolves this issue.

B.8. cluster

B.8.1. RHBA-2011:1178 – 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 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 Fix

BZ#681027

Due to an incorrect call of a function from the libxml2 library, each update of cluster configuration caused the configuration library to leak a small amount of memory. This update applies a patch that removes this incorrect function call, and updating cluster configuration no longer leads to memory leaks.

All users of Red Hat High Availability and Red Hat Resilient Storage are advised to upgrade to these updated packages, which fix this bug.

B.8.2. RHBA-2011:0361 – cluster and gfs2-utils bug fix update

Updated cluster and gfs2-utils packages that fix a bug 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 Fix

BZ#643279

Due to an incorrect conversion of directory inodes with the height larger than 1, running the gfs2_convert utility on a file system with extremely large directories may have caused the file system to become corrupted. With this update, the underlying source code has been modified to target this issue, and the gfs2_convert utility now works as expected.

All users of Red Hat High Availability and Red Hat Resilient Storage are advised to upgrade to these updated packages, which resolve this issue.

B.8.3. RHBA-2010:0844 – cluster and gfs2-utils bug fix update

Updated cluster and gfs2-utils packages that fix several bugs 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#634201

The /proc/mounts file system is no longer updated with the wrong device.

BZ#638954

A 'service cman stop remove' command no longer erroneously and permanently sets the 'remove' flag for a node for every subsequent stop/leave operation.

BZ#639958

When two cluster nodes attempt to form a cluster with different configuration files, the one with the more recent version no longer gets killed.

BZ#637699

The fsck.gfs2 utility no longer crashes if journals are missing.

All users of Red Hat High Availability and Red Hat Resilient Storage are advised to upgrade to these updated packages, which address these issues.

B.9. compat-dapl

B.9.1. RHBA-2011:0343 – compat-dapl bug fix update

Updated compat-dapl packages that fix a bug are now available for Red Hat Enterprise Linux 6.

The DAT programming API provides a means of utilizing high performance network technologies, such as InfiniBand and iWARP, without needing to write your program to use those technologies directly. This package contains the libraries that implement version 1.2 of the DAT API. The current (and recommended version for any new code) is 2.0. These 1.2 libraries are provided solely for backward compatibility.

Bug Fix

BZ#673992

Under certain error conditions, an error in the code path in compat-dapl did not allow the cp_ptr entry to be cleaned up correctly in the internal link list. This could cause new connections to fail. This update includes a backported fix from uDAPL 2.0 which ensures the entry is cleaned up correctly and subsequent connections work as expected.

Users should upgrade to these updated packages, which fix this bug.

B.10. corosync

B.10.1. RHBA-2012:1216 – 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#850681

Previously, a bug in the Corosync server caused that when an IPC (inter-process communication) connection exited or was terminated, Corosync failed to free the memory for this connection. Consequently, Corosync memory could grow. This update fixes this bug and Corosync now always frees IPC memory as expected in the described scenario.

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

B.10.2. RHBA-2012:0735 – 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#828430

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.

B.10.3. RHBA-2012:0534 – 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 the C language APIs for Red Hat Enterprise Linux cluster software.

Bug Fix

BZ#810915

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.

B.10.4. RHBA-2012:0374 – 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#791234

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.

B.10.5. RHBA-2011:1363 – corosync bug fix update

Updated corosync packages that fix several bugs 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 Fixes

BZ#726607

Previously, under heavy traffic, receive buffers sometimes overflowed, causing loss of packets. Consequently, retransmit list error messages appeared in the log files. This bug has been fixed, incoming messages are now processed more frequently, and the retransmit list error messages no longer appear in the described scenario.

BZ#727960

Previously, when a combination of a lossy network and a large number of configuration changes was used with corosync, corosync sometimes terminated unexpectedly. This bug has been fixed, and corosync no longer crashes in the described scenario.

BZ#734996

Prior to this update, when corosync ran the "cman_tool join" and "cman_tool leave" commands in a loop, corosync sometimes terminated unexpectedly. This bug has been fixed, and corosync no longer crashes in the described scenario.

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

B.10.6. RHBA-2011:0854 – corosync bug fix update

Updated corosync packages that fix several bugs 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 Fixes

BZ#696735

When the corosync server terminated unexpectedly, if it was connected to corosync clients, a shared memory leak occurred. This bug has been fixed and no memory leaks occur in the described scenario.

BZ#696734

When a ring ID file was smaller than 8 bytes, the corosync server terminated unexpectedly. With this update, if no proper ring ID file can be loaded, the corosync server creates one and no crash will occur.

BZ#696733

During the recovery phase, the corosync server sometimes terminated unexpectedly. As a consequence, a network token was lost and new configuration had to be created. This bug has been fixed and the corosync server no longer crashes in the described scenario.

BZ#696732

In rare circumstances involving multiple running nodes, the corosync server terminated unexpectedly during shut down. This bug has been fixed and the corosync server no longer crashes.

BZ#681258

When inconsistent cluster.conf files with different versions were used among nodes, a memory leak occurred in the corosync server during the configuration reload. This bug has been fixed and the configuration reload via the cman_tool no longer causes memory leaks.

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

B.10.7. RHBA-2011:0360 – corosync bug fix update

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

[Update 18 August 2011] The channel mappings in this erratum have been updated. No changes have been made to the packages.

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

Bug Fix

BZ#683592

Compared to a unicast token, certain network switches add an extra delay to the transmission of a multicast packet. Consequent to this, multicast messages may have been retransmitted, even though the message was not lost and the retransmission was therefore not necessary. This update introduces the "miss_count_const" constant that allows a user to specify the maximum number of times a message is checked for retransmission before the retransmission is performed.

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

B.11. cups

B.11.1. RHSA-2010:0866 – Important: cups security update

Updated cups 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.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems.

CVE-2010-2941

An invalid free flaw was found in the way the CUPS server parsed Internet Printing Protocol (IPP) packets. A malicious user able to send IPP requests to the CUPS server could use this flaw to crash the CUPS server.

Red Hat would like to thank Emmanuel Bouillon of NATO C3 Agency for reporting this issue.

Users of cups are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, the cupsd daemon will be restarted automatically.

B.12. cvs

B.12.1. RHSA-2010:0918 – Moderate: cvs security update

An updated cvs 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.

Concurrent Version System (CVS) is a version control system that can record the history of your files.

CVE-2010-3846

An array index error, leading to a heap-based buffer overflow, was found in the way CVS applied certain delta fragment changes from input files in the RCS (Revision Control System file) format. If an attacker in control of a CVS repository stored a specially-crafted RCS file in that repository, and then tricked a remote victim into checking out (updating their CVS repository tree) a revision containing that file, it could lead to arbitrary code execution with the privileges of the CVS server process on the system hosting the CVS repository.

Red Hat would like to thank Ralph Loader for reporting this issue.

All users of cvs are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

B.13. dapl

B.13.1. RHBA-2011:0354 – dapl bug fix and enhancement update

Updated dapl packages that fix several bugs and add provider entries to the dat.conf are now available.

dapl provides a userspace implementation of the DAT 2.0 API and is built to natively support InfiniBand and iWARP network technology.

Bug Fixes

BZ#673989

Under certain error conditions dapl did not allow the cp_ptr entry to be cleaned up correctly in the internal link list. This could cause new connections to fail. With this update, the entry is cleaned up correctly and subsequent connections work as expected.

BZ#673993

Under certain error conditions dapl could fail to free allocated memory. The consequent memory leak could, potentially, result in an out of memory condition for the application. This update frees allocated memory correctly, closing the leak.

BZ#675198

Under certain circumstances, when a thread was waiting on dapls_evd_dto_wait() and the thread received a signal, the function would return an incorrect error code, resulting in the application failing rather than retrying the request.

BZ#675205

On systems with multiple InfiniBand (IB) adapters, especially if some were configured and some not, the dat_ia_open() function could hang when the driver queried the IB devices listed in /etc/dat.conf. This primarily presented as IBM DB2 installations hanging before they completed. With this update, the dat_ia_open() hang has been fixed and IBM DB2 installations, in particular, now succeed as expected.

Enhancement

BZ#675202

New provider entries for Mellanox RDMA over Converged Ethernet (RoCE) devices were added to the dat.conf file.

Users should upgrade to these updated packages, which fix these issues.

B.14. dbus

B.14.1. RHSA-2011:0376 – Moderate: dbus security update

Updated dbus 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.

D-Bus is a system for sending messages between applications. It is used for the system-wide message bus service and as a per-user-login-session messaging facility.

CVE-2010-4352

A denial of service flaw was discovered in the system for sending messages between applications. A local user could send a message with an excessive number of nested variants to the system-wide message bus, causing the message bus (and, consequently, any process using libdbus to receive messages) to abort.

All users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. For the update to take effect, all running instances of dbus-daemon and all running applications using the libdbus library must be restarted, or the system rebooted.

B.15. device-mapper-multipath

B.15.1. RHBA-2011:1485 – device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix one bug are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

Bug Fix

BZ#751079

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 multipathd daemon now aborts any path checks when the multipath device is removed and the problem no longer occurs.

All users of device-mapper-multipath are advised to upgrade to these updated packages, which fix this bug.

B.15.2. RHBA-2011:0831 – device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath utility provides tools to manage multipath devices by giving the "dm-multipath" kernel module instructions on what to do, as well as by managing the creation and removal of partitions for device-mapper devices.

Bug Fixes

BZ#696133

Previously, multipath marked paths as failed if it could not determine whether the path was offline through sysfs. With this update, multipath calls the path_checker function to get the path's state when it cannot be determined.

BZ#702402

Previously, the multipath daemon did not remove restored paths correctly when one dervice path came online after another device path failed. Due to this issue, the multipath daemon could terminate unexpectedly with a segmentation fault on a multipath device when the path_grouping_policy option was set to the group_by_prio value. With this update multipath removes and restores such paths correctly.

All users of device-mapper-multipath are advised to upgrade to these updated packages, which fix these bugs.

B.15.3. RHBA-2011:0384 – device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the "dm-multipath" kernel module instructions on what to do, as well as by managing the creation and removal of partitions for Device-Mapper devices.

Bug Fix

BZ#684684

Prior to this update, multipathd did not always remove a path's sysfs device from cache when the path was removed. Also, multipathd searched the cache and created sysfs devices without the 'vecs' lock held. As a result, paths would occasionally have invalid sysfs devices, causing multipathd crashes and other errors. With this update, multipathd always removes the sysfs device from cache when deleting the path, and it only accesses the cache with the 'vecs' lock held.

All users of device-mapper-multipath are advised to upgrade to these updated packages, which resolve this issue.

B.15.4. RHBA-2011:0294 – device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the "dm-multipath" kernel module instructions on what to do, as well as by managing the creation and removal of partitions for Device-Mapper devices.

Bug Fix

BZ#672151

Multipathd caches the value of sysfs attribute lookups for the path devices that make up a multipath device. Previously, these weren't being removed when the path devices were removed. As well, in some cases the cache was not helpful and not used. This occasionally caused memory leaks when path devices were removed and restored. With this update, the unnecessary caching has been completely removed and the cached values are now removed when the corresponding path device is removed. Consequently, the occasional memory leaks no longer occur.

All device-mapper-multipath users are advised to upgrade to these updated packages, which resolve this issue.

B.15.5. RHBA-2011:0173 – device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the "dm-multipath" kernel module instructions on what to do, as well as by managing the creation and removal of partitions for Device-Mapper devices.

Bug Fix

BZ#658937

When all paths of a pathgroup with set group_by_prio were restored after a failure, multipathd could place some paths into a wrong pathgroup. This issue occurred, because the daemon checked if pathgroups needed reconfiguration only if a path priority changed. When the original paths were restored, they could have been assigned the same priority as before the failure. In such case the paths were incorrectly left in a wrong pathgroup. With this update, when checking if it needs to recalculate the pathgroups, the multipathd daemon refreshes and checks all priorities once a new path becomes available and places recovered paths into the correct pathgroup.

All users of device-mapper-multipath are advised to upgrade to these updated packages, which resolve this issue.

B.16. dhcp

B.16.1. RHSA-2010:0923 – 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. DHCPv6 is the DHCP protocol version for IPv6 networks.

CVE-2010-3611

A NULL pointer dereference flaw was discovered in the way the dhcpd daemon parsed DHCPv6 packets. A remote attacker could use this flaw to crash dhcpd via a specially-crafted DHCPv6 packet, if dhcpd was running as a DHCPv6 server.

Users running dhcpd as a DHCPv6 server 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.

B.16.2. RHSA-2011:0256 – 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. DHCPv6 is the DHCP protocol version for IPv6 networks.

CVE-2011-0413

A flaw was found in the way the dhcpd daemon processed certain DHCPv6 messages for addresses that had previously been declined and marked as abandoned internally. If a remote attacker sent such messages to dhcpd, it could cause dhcpd to crash due to an assertion failure if it was running as a DHCPv6 server.

Red Hat would like to thank Internet Systems Consortium for reporting this issue.

Users running dhcpd as a DHCPv6 server 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.

B.16.3. RHSA-2011:0428 – Important: dhcp security update

Updated dhcp 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 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.

CVE-2011-0997

It was discovered that the DHCP client daemon, dhclient, did not sufficiently sanitize certain options provided in DHCP server replies, such as the client hostname. A malicious DHCP server could send such an option with a specially-crafted value to a DHCP client. If this option's value was saved on the client system, and then later insecurely evaluated by a process that assumes the option is trusted, it could lead to arbitrary code execution with the privileges of that process.

Red Hat would like to thank Sebastian Krahmer of the SuSE Security Team for reporting this issue.

All dhclient users should upgrade to these updated packages, which contain a backported patch to correct this issue.

B.17. dmidecode

B.17.1. RHBA-2011:1396 – dmidecode bug fix update

An updated dmidecode package that fixes one bug is now available for Red Hat Enterprise Linux 6 Extended Update Support.

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.

Bug Fix

BZ#745558

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.

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

B.18. dracut

B.18.1. RHEA-2011:0141 – dracut enhancement update

Updated dracut packages that add an enhancement are now available for Red Hat Enterprise Linux 6.

The dracut packages provide an event-driven initramfs generator infrastructure based around udev. The initramfs is loaded together with the kernel at boot time and initializes the system, so it can read and boot from the root partition.

Enhancement

BZ#661298

The dracut packages have been updated to support the new kernel boot option, "rdinsmodpost=[module]", which allows a user to specify a kernel module to be loaded after all device drivers are loaded automatically.

Users of dracut are advised to upgrade to these updated packages, which add this enhancement.

B.18.2. RHBA-2010:0877 – dracut bug fix update

Updated dracut packages that fix a bug are now available for Red Hat Enterprise Linux 6.

The dracut package is an event-driven initramfs generator infrastructure based around udev. The 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#651402

Prior to this update, the udev rules used by dracut may have caused the merged logical volume management (LVM) snapshots to be accessed. Consequent to this, I/O errors appeared in the log. With this update, dracut's internal udev rules have been updated to ignore those internal devices, and dracut now works as expected.

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

B.19. evince

B.19.1. RHSA-2011:0009 – Moderate: evince security update

Updated evince 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Evince is a document viewer.

CVE-2010-2640, CVE-2010-2641

An array index error was found in the DeVice Independent (DVI) renderer's PK and VF font file parsers. A DVI file that references a specially-crafted font file could, when opened, cause Evince to crash or, potentially, execute arbitrary code with the privileges of the user running Evince.

CVE-2010-2642

A heap-based buffer overflow flaw was found in the DVI renderer's AFM font file parser. A DVI file that references a specially-crafted font file could, when opened, cause Evince to crash or, potentially, execute arbitrary code with the privileges of the user running Evince.

CVE-2010-2643

An integer overflow flaw was found in the DVI renderer's TFM font file parser. A DVI file that references a specially-crafted font file could, when opened, cause Evince to crash or, potentially, execute arbitrary code with the privileges of the user running Evince.

Note: The above issues are not exploitable unless an attacker can trick the user into installing a malicious font file.

Red Hat would like to thank the Evince development team for reporting these issues. Upstream acknowledges Jon Larimer of IBM X-Force as the original reporter of these issues.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues.

B.20. fence-agents

B.20.1. RHBA-2011:0363 – fence-agents bug fix update

An updated fence-agents package that fixes a 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#680522

A bug fix for a previous advisory, the RHEA-2010:0904 enhancement update, stated that the Brocade 200E, Brocade 300, Brocade 4100, Brocade 4900, and Brocade 5100 fencing devices are now supported by the fence_brocade agent. However, the fence_brocade agent was not included in the updated package. This update corrects this error, and the fence_brocade agent is now included in the package as expected.

All users of fence-agents are advised to upgrade to this updated package, which resolves this issue.

B.20.2. RHEA-2010:0904 – fence-agents enhancement update

An updated fence-agents package that adds support for new hardware and Red Hat Enterprise Virtualization is now available.

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.

Enhancements

BZ#642695

The package has been updated to provide a fencing agent that is able to communicate with Red Hat Enterprise Virtualization Manager, allowing virtual machines to be fenced.

BZ#643340

For Intelligent Platform Management Interface (IPMI) devices, the "power_wait" delay can now be adjusted in order to support newer iLO 3 firmware.

BZ#643515

Brocade 200E, Brocade 300, Brocade 4100, Brocade 4900, and Brocade 5100 fencing devices are now supported by the fence_brocade agent, and can be used with both Red Hat High Availability and Red Hat Resilient Storage.

All users requiring any of the features listed above are advised to upgrade to this new package, which adds these enhancements.

B.21. firefox

B.21.1. RHSA-2010:0861 – Critical: firefox security update

Updated firefox 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 scores, 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.

CVE-2010-3765

A race condition flaw was found in the way Firefox handled Document Object Model (DOM) element properties. Malicious HTML content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2010-3175, CVE-2010-3176, CVE-2010-3179, CVE-2010-3183, CVE-2010-3180

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-2010-3177

A flaw was found in the way the Gopher parser in Firefox converted text into HTML. A malformed file name on a Gopher server could, when accessed by a victim running Firefox, allow arbitrary JavaScript to be executed in the context of the Gopher domain.

CVE-2010-3178

A same-origin policy bypass flaw was found in Firefox. An attacker could create a malicious web page that, when viewed by a victim, could steal private data from a different website the victim had loaded with Firefox.

CVE-2010-3182

A flaw was found in the script that launches Firefox. The LD_LIBRARY_PATH variable was appending a "." character, which could allow a local attacker to execute arbitrary code with the privileges of a different user running Firefox, if that user ran Firefox from within an attacker-controlled directory.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.11 and 3.6.12:

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.11

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.12

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.12, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

B.21.2. RHSA-2010:0966 – Critical: firefox security update

Updated firefox packages that fix several 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 scores, 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.

CVE-2010-3766, **CVE-2010-3767**, **CVE-2010-3772**, **CVE-2010-3776**, **CVE-2010-3777**

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-2010-3771

A flaw was found in the way Firefox handled malformed JavaScript. A website with an object containing malicious JavaScript could cause Firefox to execute that JavaScript with the privileges of the user running Firefox.

CVE-2010-3768

This update adds support for the Sanitiser for OpenType (OTS) library to Firefox. This library helps prevent potential exploits in malformed OpenType fonts by verifying the font file prior to use.

CVE-2010-3775

A flaw was found in the way Firefox loaded Java LiveConnect scripts. Malicious web content could load a Java LiveConnect script in a way that would result in the plug-in object having elevated privileges, allowing it to execute Java code with the privileges of the user running Firefox.

CVE-2010-3773

It was found that the fix for CVE-2010-0179 was incomplete when the Firebug add-on was used. If a user visited a website containing malicious JavaScript while the Firebug add-on was enabled, it could cause Firefox to execute arbitrary JavaScript with the privileges of the user running Firefox.

CVE-2010-3774

A flaw was found in the way Firefox presented the location bar to users. A malicious website could trick a user into thinking they are visiting the site reported by the location bar, when the page is actually content controlled by an attacker.

CVE-2010-3770

A cross-site scripting (XSS) flaw was found in the Firefox x-mac-arabic, x-mac-farsi, and x-mac-hebrew character encodings. Certain characters were converted to angle brackets when displayed. If server-side script filtering missed these cases, it could result in Firefox executing JavaScript code with the permissions of a different website.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.13:

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.13

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.13, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

B.21.3. RHSA-2011:0310 – Critical: firefox security and bug fix update

Updated firefox packages that fix several security issues and one bug 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 scores, 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.

CVE-2010-1585

A flaw was found in the way Firefox sanitized HTML content in extensions. If an extension loaded or rendered malicious content using the ParanoidFragmentSink class, it could fail to safely display the content, causing Firefox to execute arbitrary JavaScript with the privileges of the user running Firefox.

CVE-2011-0051

A flaw was found in the way Firefox handled dialog boxes. An attacker could use this flaw to create a malicious web page that would present a blank dialog box that has non-functioning buttons. If a user closes the dialog box window, it could unexpectedly grant the malicious web page elevated privileges.

CVE-2011-0053, CVE-2011-0055, CVE-2011-0058, CVE-2011-0062

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-2011-0054, CVE-2011-0056, CVE-2011-0057

Several flaws were found in the way Firefox handled malformed JavaScript. A website containing malicious JavaScript could cause Firefox to execute that JavaScript with the privileges of the user running Firefox.

CVE-2011-0061

A flaw was found in the way Firefox handled malformed JPEG images. A website containing a malicious JPEG image could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-0059

A flaw was found in the way Firefox handled plug-ins that perform HTTP requests. If a plug-in performed an HTTP request, and the server sent a 307 redirect response, the plug-in was not notified, and the HTTP request was forwarded. The forwarded request could contain custom headers, which could result in a Cross Site Request Forgery attack.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.14:

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.14

Bug Fix

BZ#463131, BZ#665031

On Red Hat Enterprise Linux 4 and 5, running the "firefox -setDefaultBrowser" command caused warnings such as the following:

> libgnomevfs-WARNING **: Deprecated function. User modifications to the MIME database are no longer supported.

This update disables the "setDefaultBrowser" option. Red Hat Enterprise Linux 4 users wishing to set a default web browser can use Applications -> Preferences -> More Preferences -> Preferred Applications. Red Hat Enterprise Linux 5 users can use System -> Preferences -> Preferred Applications.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.14, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

B.21.4. RHSA-2011:0373 – Important: firefox security update

Updated firefox 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.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Issue

BZ#689430

This erratum blacklists a small number of HTTPS certificates.

All Firefox users should upgrade to these updated packages, which contain a backported patch. After installing the update, Firefox must be restarted for the changes to take effect.

B.21.5. RHSA-2011:0471 – Critical: firefox security update

Updated firefox packages that fix several 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 scores, 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.

CVE-2011-0080, CVE-2011-0081

Several flaws were found in the processing of malformed web content. A web page containing malicious content could possibly lead to arbitrary code execution with the privileges of the user running Firefox.

CVE-2011-0078

An arbitrary memory write flaw was found in the way Firefox handled out-of-memory conditions. If all memory was consumed when a user visited a malicious web page, it could possibly lead to arbitrary code execution with the privileges of the user running Firefox.

CVE-2011-0077

An integer overflow flaw was found in the way Firefox handled the HTML frameset tag. A web page with a frameset tag containing large values for the "rows" and "cols" attributes could trigger this flaw, possibly leading to arbitrary code execution with the privileges of the user running Firefox.

CVE-2011-0075

A flaw was found in the way Firefox handled the HTML iframe tag. A web page with an iframe tag containing a specially-crafted source address could trigger this flaw, possibly leading to arbitrary code execution with the privileges of the user running Firefox.

CVE-2011-0074

A flaw was found in the way Firefox displayed multiple marquee elements. A malformed HTML document could cause Firefox to execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-0073

A flaw was found in the way Firefox handled the nsTreeSelection element. Malformed content could cause Firefox to execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-0072

A use-after-free flaw was found in the way Firefox appended frame and iframe elements to a DOM tree when the NoScript add-on was enabled. Malicious HTML content could cause Firefox to execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-0071

A directory traversal flaw was found in the Firefox resource:// protocol handler. Malicious content could cause Firefox to access arbitrary files accessible to the user running Firefox.

CVE-2011-0070

A double free flaw was found in the way Firefox handled "application/http-index-format" documents. A malformed HTTP response could cause Firefox to execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-0069

A flaw was found in the way Firefox handled certain JavaScript cross-domain requests. If malicious content generated a large number of cross-domain JavaScript requests, it could cause Firefox to execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-0067

A flaw was found in the way Firefox displayed the autocomplete pop-up. Malicious content could use this flaw to steal form history information.

CVE-2011-0066, CVE-2011-0065

Two use-after-free flaws were found in the Firefox mObserverList and mChannel objects. Malicious content could use these flaws to execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-1202

A flaw was found in the Firefox XSLT generate-id() function. This function returned the memory address of an object in memory, which could possibly be used by attackers to bypass address randomization protections.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.17.

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.17

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.17, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

B.22. flash-plugin

B.22.1. RHSA-2010:0867 – Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

CVE-2010-3639, CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, CVE-2010-3652, CVE-2010-3654

This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed on the Adobe security page APSB10-26.

Multiple security flaws were found in the way flash-plugin displayed certain SWF content. An attacker could use these flaws to create a specially-crafted SWF file that would cause flash-plugin to crash or, potentially, execute arbitrary code when the victim loaded a page containing the specially-crafted SWF content.

CVE-2010-3636

An input validation flaw was discovered in flash-plugin. Certain server encodings could lead to a bypass of cross-domain policy file restrictions, possibly leading to cross-domain information disclosure.

During testing, it was discovered that there were regressions with Flash Player on certain sites, such as fullscreen playback on YouTube. Despite these regressions, we feel these security flaws are serious enough to update the package with what Adobe has provided.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.1.102.64.

B.23. freetype

B.23.1. RHSA-2010:0864 – Important: freetype security update

Updated freetype 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 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. These packages provide the FreeType 2 font engine.

CVE-2010-2805, CVE-2010-3311

It was found that the FreeType font rendering engine improperly validated certain position values when processing input streams. If a user loaded a specially-crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

CVE-2010-2808

A stack-based buffer overflow flaw was found in the way the FreeType font rendering engine processed some PostScript Type 1 fonts. If a user loaded a specially-crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

CVE-2010-2806

An array index error was found in the way the FreeType font rendering engine processed certain PostScript Type 42 font files. If a user loaded a specially-crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Note: All of the issues in this erratum only affect the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

B.23.2. RHSA-2010:0889 – Important: freetype security update

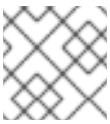
Updated freetype packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

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. The freetype packages for Red Hat Enterprise Linux 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 and 6 provide only the FreeType 2 font engine.

CVE-2010-3855

A heap-based buffer overflow flaw was found in the way the FreeType font rendering engine processed certain TrueType GX fonts. If a user loaded a specially-crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.



NOTE

Note: This issue only affects the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. The X server must be restarted (log out, then log back in) for this update to take effect.

B.24. gdb

B.24.1. RHBA-2011:0145 – gdb bug fix update

Updated gdb packages that fix a bug are now available for Red Hat Enterprise Linux 6.

The GNU debugger, gdb, allows the debugging of programs written in C, C++, and other languages by executing them in a controlled fashion and then printing out their data.

Bug Fix

BZ#662218

After you issued the command 'info program', GDB could have terminated unexpectedly, because a change of the shared library list corrupted the data in the internal GDB structure 'bpstat'. With this update, the 'bpstat' structure contains after a change in the shared library list the correct data and the command 'info program' works as expected.

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

B.25. gdm

B.25.1. RHSA-2011:0395 – Moderate: gdm security update

Updated gdm 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 GNOME Display Manager (GDM) provides the graphical login screen, shown shortly after boot up, log out, and when user-switching.

CVE-2011-0727

A race condition flaw was found in the way GDM handled the cache directories used to store users' dmrc and face icon files. A local attacker could use this flaw to trick GDM into changing the ownership of an arbitrary file via a symbolic link attack, allowing them to escalate their privileges.

Red Hat would like to thank Sebastian Krahmer of the SuSE Security Team for reporting this issue.

All users should upgrade to these updated packages, which contain a backported patch to correct this issue. GDM must be restarted for this update to take effect. Rebooting achieves this, but changing the runlevel from 5 to 3 and back to 5 also restarts GDM.

B.26. git

B.26.1. RHSA-2010:1003 – Moderate: git security update

Updated git 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.

Git is a fast, scalable, distributed revision control system.

CVE-2010-3906

A cross-site scripting (XSS) flaw was found in gitweb, a simple web interface for Git repositories. A remote attacker could perform an XSS attack against victims by tricking them into visiting a specially-crafted gitweb URL.

All gitweb users should upgrade to these updated packages, which contain a backported patch to correct this issue.

B.27. glibc

B.27.1. RHSA-2010:0872 – Important: glibc security and bug fix update

Updated glibc packages that fix two security issues and two 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. 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.

CVE-2010-3847

It was discovered that the glibc dynamic linker/loader did not handle the $ORIGIN dynamic string token set in the LD_AUDIT environment variable securely. A local attacker with write access to a file system containing setuid or setgid binaries could use this flaw to escalate their privileges.

CVE-2010-3856

It was discovered that the glibc dynamic linker/loader did not perform sufficient safety checks when loading dynamic shared objects (DSOs) to provide callbacks for its auditing API during the execution of privileged programs. A local attacker could use this flaw to escalate their privileges via a carefully-chosen system DSO library containing unsafe constructors.

Red Hat would like to thank Tavis Ormandy for reporting the CVE-2010-3847 issue, and Ben Hawkes and Tavis Ormandy for reporting the CVE-2010-3856 issue.

Bug Fixes

BZ#643341

Previously, the generic implementation of the strstr() and memmem() functions did not handle certain periodic patterns correctly and could find a false positive match. This error has been fixed, and both functions now work as expected.

BZ#643343

The "TCB_ALIGNMENT" value has been increased to 32 bytes to prevent applications from crashing during symbol resolution on 64-bit systems with support for Intel AVX vector registers.

All users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

B.27.2. RHSA-2011:0413 — Important: glibc security update

Updated glibc packages that fix three 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 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.

CVE-2011-0536

The fix for CVE-2010-3847 introduced a regression in the way the dynamic loader expanded the $ORIGIN dynamic string token specified in the RPATH and RUNPATH entries in the ELF library header. A local attacker could use this flaw to escalate their privileges via a setuid or setgid program using such a library.

CVE-2011-1071

It was discovered that the glibc fnmatch() function did not properly restrict the use of alloca(). If the function was called on sufficiently large inputs, it could cause an application using fnmatch() to crash or, possibly, execute arbitrary code with the privileges of the application.

CVE-2011-1095

It was discovered that the locale command did not produce properly escaped output as required by the POSIX specification. If an attacker were able to set the locale environment variables in the environment of a script that performed shell evaluation on the output of the locale command, and that script were run with different privileges than the attacker's, it could execute arbitrary code with the privileges of the script.

All users should upgrade to these updated packages, which contain backported patches to correct these issues.

B.27.3. RHBA-2011:1180 — glibc bug fix update

Updated glibc packages that fix several bugs are now available for Red Hat Enterprise Linux 6 Extended Update Support.

The glibc packages contain the standard C and the standard math libraries. These libraries are used by multiple programs on the system, and without these libraries, the Linux system cannot function properly.

Bug Fixes

BZ#712124

Under certain circumstances, a threaded process could have been granted incomplete group membership of the user who was running the process. This was caused by glibc using its default method for group membership determination, which led to the situation where multiple threads interfered with each other while attempting to retrieve the information simultaneously. Due to the nature of the group membership determination method used, each thread ended up with a different subset of the entire result set. With this update, the group membership determination method has been modified to precede this interference.

BZ#712406

When a process corrupted its heap, the malloc() function could have entered a deadlock situation while building up an error message string. This caused the process unresponsive. With this update, the code has been modified to use the mmap() function to allocate memory for the error message. This workaround ensures that malloc() deadlock no longer occurs when allocating memory for an error message when the corrupted process heap is detected, and such a process is now normally aborted.

BZ#715386

Previously, nscd did not take into consideration time-to-live (TTL) parameters for the DNS records it was caching. With this update, the code has been modified so that nscd now respects TTL parameters when it answers requests for DNS records.

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

B.27.4. RHBA-2011:0321 – glibc bug fix update

Updated glibc packages that fix a bug in the dynamic linker are now available for Red Hat Enterprise Linux 6.

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.

Bug Fix

BZ#661396

Due to an error in glibc libraries, a race condition could occur when traversing a list of currently loaded shared libraries, causing an application to terminate with an error. This error has been fixed, the race condition no longer occurs, and the list of shared libraries can now be traversed as expected.

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

B.28. gpxe

B.28.1. RHBA-2011:0415 – 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#680148

Previously, the virtIO gPXE driver padded all packets to maximum length. This could confuse some gateways because the Ethernet standard is to pad only packets of up to 64 bytes in length. Due to this issue, virtual machines with a virtIO NIC (network interface card) failed to connect to the PXE server behind a gateway. Subsequently, the PXE boot failed. This update pads only packets of up to 64 bytes in length. Now, virtual machines with a virtIO NIC connect to the same PXE server without further problems.

All gPXE users are advised to upgrade to these updated packages which fix this bug.

B.29. hplip

B.29.1. RHSA-2011:0154 – Moderate: hplip security update

Updated hplip 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.

Hewlett-Packard Linux Imaging and Printing (HPLIP) provides drivers for Hewlett-Packard printers and multifunction peripherals, and tools for installing, using, and configuring them.

CVE-2010-4267

A flaw was found in the way certain HPLIP tools discovered devices using the SNMP protocol. If a user ran certain HPLIP tools that search for supported devices using SNMP, and a malicious user is able to send specially-crafted SNMP responses, it could cause those HPLIP tools to crash or, possibly, execute arbitrary code with the privileges of the user running them.

Red Hat would like to thank Sebastian Krahmer of the SuSE Security Team for reporting this issue.

Users of hplip should upgrade to these updated packages, which contain a backported patch to correct this issue.

B.30. initscripts

B.30.1. RHBA-2010:1004 – initscripts bug fix update

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

The initscripts package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

Bug Fix

BZ#660327

Prior to this update, users were unable to set the VLAN tag to 0 when creating a logical network. With this update, the ifup script has been updated to permit this value, and the VLAN identification number can now be set to 0 as expected.

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

B.31. java-1.5.0-ibm

B.31.1. RHSA-2011:0364 – 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 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 scores, 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.

CVE-2010-4447, CVE-2010-4448, CVE-2010-4450, CVE-2010-4454, CVE-2010-4462, CVE-2010-4465, CVE-2010-4466, CVE-2010-4468, CVE-2010-4471, CVE-2010-4473, CVE-2010-4475

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 SR12-FP4 Java release. All running instances of IBM Java must be restarted for this update to take effect.

B.31.2. RHSA-2011:0291 – Moderate: java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix one security issue 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 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 IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

CVE-2010-4476

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Java based applications to hang, for example, if they parsed Double values in a specially-crafted HTTP request.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.5.0 SR12-FP3 Java release. All running instances of IBM Java must be restarted for this update to take effect.

B.31.3. RHSA-2011:0169 — Critical: java-1.5.0-ibm security and bug fix update

Updated java-1.5.0-ibm packages that fix multiple security issues and one bug 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 scores, 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.

CVE-2010-3553, CVE-2010-3557, CVE-2010-3571

This update fixes multiple 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.

Bug Fix

BZ#659710

An error in the java-1.5.0-ibm RPM spec file caused an incorrect path to be included in HtmlConverter, preventing it from running.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.5.0 SR12-FP3 Java release. All running instances of IBM Java must be restarted for this update to take effect.

B.31.4. RHSA-2010:0873 — 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 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, 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.

CVE-2010-1321, CVE-2010-3541, CVE-2010-3548, CVE-2010-3549, CVE-2010-3550, CVE-2010-3551, CVE-2010-3556, CVE-2010-3559, CVE-2010-3562, CVE-2010-3565, CVE-2010-3566, CVE-2010-3568, CVE-2010-3569, CVE-2010-3572, CVE-2010-3573, CVE-2010-3574

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 SR12-FP2 Java release. All running instances of IBM Java must be restarted for this update to take effect.

B.32. java-1.6.0-ibm

B.32.1. RHSA-2011:0357 – 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM 1.6.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

CVE-2010-4422, CVE-2010-4447, CVE-2010-4448, CVE-2010-4452, CVE-2010-4454, CVE-2010-4462, CVE-2010-4463, CVE-2010-4465, CVE-2010-4466, CVE-2010-4467, CVE-2010-4468, CVE-2010-4471, CVE-2010-4473, CVE-2010-4475

> 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.

Note: The RHSA-2010:0987 and RHSA-2011:0290 java-1.6.0-ibm errata were missing 64-bit PowerPC packages for Red Hat Enterprise Linux 4 Extras. This erratum provides 64-bit PowerPC packages for Red Hat Enterprise Linux 4 Extras as expected.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR9-FP1 Java release. All running instances of IBM Java must be restarted for the update to take effect.

B.32.2. RHSA-2011:0290 – Moderate: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix one security issue 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 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 IBM 1.6.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

CVE-2010-4476

> A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Java based applications to hang, for example, if they parsed Double values in a specially-crafted HTTP request.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR9 Java release. All running instances of IBM Java must be restarted for the update to take effect.

B.32.3. RHSA-2010:0987 – Critical: java-1.6.0-ibm security and bug fix update

Updated java-1.6.0-ibm packages that fix several security issues and two bugs 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM 1.6.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

CVE-2009-3555, CVE-2010-1321, CVE-2010-3541, CVE-2010-3548, CVE-2010-3549, CVE-2010-3550, CVE-2010-3551, CVE-2010-3553, CVE-2010-3555, CVE-2010-3556, CVE-2010-3557, CVE-2010-3558, CVE-2010-3560, CVE-2010-3562, CVE-2010-3563, CVE-2010-3565, CVE-2010-3566, CVE-2010-3568, CVE-2010-3569, CVE-2010-3571, CVE-2010-3572, CVE-2010-3573, CVE-2010-3574

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page.

Bug Fixes

BZ#659716

An error in the java-1.6.0-ibm RPM spec file caused an incorrect path to be included in HtmlConverter, preventing it from running.

BZ#633341

On AMD64 and Intel 64 systems, if only the 64-bit java-1.6.0-ibm packages were installed, IBM Java 6 Web Start was not available as an application that could open JNLP (Java Network Launching Protocol) files. This affected file management and web browser tools. Users had to manually open them with the "/usr/lib/jvm/jre-1.6.0-ibm.x86_64/bin/javaws" command. This update resolves this issue.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR9 Java release. All running instances of IBM Java must be restarted for the update to take effect.

B.33. java-1.6.0-openjdk

B.33.1. RHSA-2010:0865 – Important: java-1.6.0-openjdk security and bug fix update

Updated java-1.6.0-openjdk packages that fix several security issues and two 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. 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.

CVE-2010-3569

defaultReadObject of the Serialization API could be tricked into setting a volatile field multiple times, which could allow a remote attacker to execute arbitrary code with the privileges of the user running the applet or application.

CVE-2010-3568

Race condition in the way objects were deserialized could allow an untrusted applet or application to misuse the privileges of the user running the applet or application.

CVE-2010-3567

Miscalculation in the OpenType font rendering implementation caused out-of-bounds memory access, which could allow remote attackers to execute code with the privileges of the user running the java process.

CVE-2010-3565

JPEGImageWriter.writeImage in the imageio API improperly checked certain image metadata, which could allow a remote attacker to execute arbitrary code in the context of the user running the applet or application.

CVE-2010-3562

Double free in IndexColorModel could cause an untrusted applet or application to crash or, possibly, execute arbitrary code with the privileges of the user running the applet or application.

CVE-2010-3561

The privileged accept method of the ServerSocket class in the Common Object Request Broker Architecture (CORBA) implementation in OpenJDK allowed it to receive connections from any host, instead of just the host of the current connection. An attacker could use this flaw to bypass restrictions defined by network permissions.

CVE-2010-3557

Flaws in the Swing library could allow an untrusted application to modify the behavior and state of certain JDK classes.

CVE-2010-3554

Flaws in the CORBA implementation could allow an attacker to execute arbitrary code by misusing permissions granted to certain system objects.

CVE-2010-3553

UIDefault.ProxyLazyValue had unsafe reflection usage, allowing untrusted callers to create objects via ProxyLazyValue values.

CVE-2010-3549

HttpURLConnection improperly handled the "chunked" transfer encoding method, which could allow remote attackers to conduct HTTP response splitting attacks.

CVE-2010-3574

HttpURLConnection improperly checked whether the calling code was granted the "allowHttpTrace" permission, allowing untrusted code to create HTTP TRACE requests.

CVE-2010-3541, CVE-2010-3573

HttpURLConnection did not validate request headers set by applets, which could allow remote attackers to trigger actions otherwise restricted to HTTP clients.

CVE-2010-3564

The Kerberos implementation improperly checked the sanity of AP-REQ requests, which could cause a denial of service condition in the receiving Java Virtual Machine.

CVE-2009-3555

The java-1.6.0-openjdk packages shipped with the GA release of Red Hat Enterprise Linux 6 mitigated a man-in-the-middle attack in the way the TLS/SSL protocols handle session renegotiation by disabling renegotiation. This update implements the TLS Renegotiation Indication Extension as defined in RFC 5746, allowing secure renegotiation between updated clients and servers.

CVE-2010-3551

The NetworkInterface class improperly checked the network "connect" permissions for local network addresses, which could allow remote attackers to read local network addresses.

CVE-2010-3548

Information leak flaw in the Java Naming and Directory Interface (JNDI) could allow a remote attacker to access information about otherwise-protected internal network names.

Note: Flaws concerning applets in this advisory (CVE-2010-3568, CVE-2010-3554, CVE-2009-3555, CVE-2010-3562, CVE-2010-3557, CVE-2010-3548, CVE-2010-3564, CVE-2010-3565, CVE-2010-3569) can only be triggered in OpenJDK by calling the "appletviewer" application.

Bug Fixes

BZ#639922

One defense in depth patch.

BZ#642779

Problems for certain SSL connections. In a reported case, this prevented the JBoss JAAS modules from connecting over SSL to Microsoft Active Directory servers.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, containing the the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit. All running instances of OpenJDK Java must be restarted for the update to take effect.

B.33.2. RHSA-2011:0214 — Moderate: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk 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. Common Vulnerability Scoring System (CVSS) base scores, 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.

CVE-2010-4476

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Java-based applications to hang, for instance if they parse Double values in a specially-crafted HTTP request.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve this issue. All running instances of OpenJDK Java must be restarted for the update to take effect.

B.33.3. RHSA-2011:0281 — Important: java-1.6.0-openjdk security and bug fix update

Updated java-1.6.0-openjdk packages that fix several 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 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.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

CVE-2010-4465

A flaw was found in the Swing library. Forged TimerEvents could be used to bypass SecurityManager checks, allowing access to otherwise blocked files and directories.

CVE-2010-4469

A flaw was found in the HotSpot component in OpenJDK. Certain bytecode instructions confused the memory management within the Java Virtual Machine (JVM), which could lead to heap corruption.

CVE-2010-4470

A flaw was found in the way JAXP (Java API for XML Processing) components were handled, allowing them to be manipulated by untrusted applets. This could be used to elevate privileges and bypass secure XML processing restrictions.

CVE-2010-4448

It was found that untrusted applets could create and place cache entries in the name resolution cache. This could allow an attacker targeted manipulation over name resolution until the OpenJDK VM is restarted.

CVE-2010-4450

It was found that the Java launcher provided by OpenJDK did not check the LD_LIBRARY_PATH environment variable for insecure empty path elements. A local attacker able to trick a user into running the Java launcher while working from an attacker-writable directory could use this flaw to load an untrusted library, subverting the Java security model.

CVE-2010-4472

A flaw was found in the XML Digital Signature component in OpenJDK. Untrusted code could use this flaw to replace the Java Runtime Environment (JRE) XML Digital Signature Transform or C14N algorithm implementations to intercept digital signature operations.

NOTE

Note that all of the above flaws can only be remotely triggered in OpenJDK by calling the "appletviewer" application.

Bug Fix

BZ#676019

This update provides one defense in depth patch.

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.

B.34. java-1.6.0-sun

B.34.1. RHSA-2011:0282 – 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 scores, 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.

CVE-2010-4422, CVE-2010-4447, CVE-2010-4448, CVE-2010-4450, CVE-2010-4451, CVE-2010-4452, CVE-2010-4454, CVE-2010-4462, CVE-2010-4463, CVE-2010-4465, CVE-2010-4466, CVE-2010-4467, CVE-2010-4468, CVE-2010-4469, CVE-2010-4470, CVE-2010-4471, CVE-2010-4472, CVE-2010-4473, CVE-2010-4475, CVE-2010-4476

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 and Java for Business Critical Patch Update Advisory page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which resolve these issues. All running instances of Sun Java must be restarted for the update to take effect.

B.35. kabi-whitelists

B.35.1. RHBA-2010:0856 – kabi-whitelists bug fix update

An updated kabi-whitelists package that fixes a bug is now available.

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.

Bug Fix

BZ#643570

Two exported kernel symbols were removed from the final version of the Kernel Application Binary Interface (kABI) whitelists package in Red Hat Enterprise Linux 6.

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

B.36. kdelibs

B.36.1. RHSA-2011:0464 – Moderate: kdelibs security update

Updated kdelibs 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

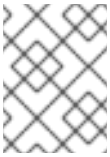
The kdelibs packages provide libraries for the K Desktop Environment (KDE).

CVE-2011-1168

A cross-site scripting (XSS) flaw was found in the way KHTML, the HTML layout engine used by KDE applications such as the Konqueror web browser, displayed certain error pages. A remote attacker could use this flaw to perform a cross-site scripting attack against victims by tricking them into visiting a specially-crafted URL.

CVE-2011-1094

A flaw was found in the way kdelibs checked the user specified hostname against the name in the server's SSL certificate. A man-in-the-middle attacker could use this flaw to trick an application using kdelibs into mistakenly accepting a certificate as if it was valid for the host, if that certificate was issued for an IP address to which the user specified hostname was resolved to.



NOTE

Note that as part of the fix, this update also introduces stricter handling for wildcards used in servers' SSL certificates.

Users should 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.

B.37. kdenetwork

B.37.1. RHSA-2011:0465 – Important: kdenetwork security update

Updated kdenetwork 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.

The kdenetwork packages contain networking applications for the K Desktop Environment (KDE).

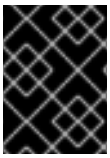
CVE-2011-1586

A directory traversal flaw was found in the way KGet, a download manager, handled the "file" element in Metalink files. An attacker could use this flaw to create a specially-crafted Metalink file that, when opened, would cause KGet to overwrite arbitrary files accessible to the user running KGet.

Users of kdenetwork should upgrade to these updated packages, which contain a backported patch to resolve this issue. The desktop must be restarted (log out, then log back in) for this update to take effect.

B.38. kernel

B.38.1. RHSA-2010:0842 – Important: kernel security and bug fix update



IMPORTANT

This update has already been released (prior to the GA of this release) as the security errata RHSA-2010:0842

Updated kernel packages that fix multiple security issues and several 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. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

[Updated 22 November 2010] The packages list in this erratum has been updated to include four missing debuginfo-common packages (one per architecture). No changes have been made to the original packages.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes
* Missing sanity checks in the Intel **i915** driver in the Linux kernel could allow a local, unprivileged user to escalate their privileges. (CVE-2010-2962, Important)

* **compat_alloc_user_space()** in the Linux kernel 32/64-bit compatibility layer implementation was missing sanity checks. This function could be abused in other areas of the Linux kernel if its length argument can be controlled from user-space. On 64-bit systems, a local, unprivileged user could use this flaw to escalate their privileges. (CVE-2010-3081, Important)

* A buffer overflow flaw in **niu_get_ethtool_tcam_all()** in the **niu** Ethernet driver in the Linux kernel, could allow a local user to cause a denial of service or escalate their privileges. (CVE-2010-3084, Important)

* A flaw in the IA32 system call emulation provided in 64-bit Linux kernels could allow a local user to escalate their privileges. (CVE-2010-3301, Important)

* A flaw in **sctp_packet_config()** in the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation could allow a remote attacker to cause a denial of service. (CVE-2010-3432, Important)

* A missing integer overflow check in **snd_ctl_new()** in the Linux kernel's sound subsystem could allow a local, unprivileged user on a 32-bit system to cause a denial of service or escalate their privileges. (CVE-2010-3442, Important)

* A flaw was found in **sctp_auth_asoc_get_hmac()** in the Linux kernel's SCTP implementation. When iterating through the ***hmac_ids*** array, it did not reset the last id element if it was out of range. This could allow a remote attacker to cause a denial of service. (CVE-2010-3705, Important)

* A function in the Linux kernel's Reliable Datagram Sockets (RDS) protocol implementation was missing sanity checks, which could allow a local, unprivileged user to escalate their privileges. (CVE-2010-3904, Important)

* A flaw in **drm_ioctl()** in the Linux kernel's Direct Rendering Manager (DRM) implementation could allow a local, unprivileged user to cause an information leak. (CVE-2010-2803, Moderate)

* It was found that wireless drivers might not always clear allocated buffers when handling a driver-specific IOCTL information request. A local user could trigger this flaw to cause an information leak. (CVE-2010-2955, Moderate)

* A NULL pointer dereference flaw in **ftrace_regex_lseek()** in the Linux kernel's ftrace implementation could allow a local, unprivileged user to cause a denial of service. Note: The debugfs file system must be mounted locally to exploit this issue. It is not mounted by default. (CVE-2010-3079, Moderate)

* A flaw in the Linux kernel's packet writing driver could be triggered via the **PKT_CTRL_CMD_STATUS** IOCTL request, possibly allowing a local, unprivileged user with access to **/dev/pktcdvd/control** to cause an information leak. Note: By default, only users in the cdrom group have access to **/dev/pktcdvd/control**. (CVE-2010-3437, Moderate)

* A flaw was found in the way KVM (Kernel-based Virtual Machine) handled the reloading of **fs** and **gs** segment registers when they had invalid selectors. A privileged host user with access to **/dev/kvm** could use this flaw to crash the host. (CVE-2010-3698, Moderate)

Red Hat would like to thank Kees Cook for reporting CVE-2010-2962 and CVE-2010-2803; Ben Hawkes for reporting CVE-2010-3081 and CVE-2010-3301; Dan Rosenberg for reporting CVE-2010-3442, CVE-2010-3705, CVE-2010-3904, and CVE-2010-3437; and Robert Swiecki for reporting CVE-2010-3079.

Bug fixes

BZ#632292

When booting a Red Hat Enterprise Linux 5.5 kernel on a guest on an AMD host system running Red Hat Enterprise Linux 6, the guest kernel crashes due to an unsupported MSR (Model Specific Registers) read of the **MSR_K7_CLK_CTL** model. With this update, KVM support was added for the **MSR_K7_CLK_CTL** model specific register used in the AMD K7 CPU models, thus, the kernel crashes no longer occur.

BZ#633864

Previously, the **s390** tape block driver crashed whenever it tried to switch the I/O scheduler. With this update, an official in-kernel API (**elevator_change()**) is used to switch the I/O scheduler safely, thus, the crashes no longer occurs.

BZ#633865

Previously, a kernel module not shipped by Red Hat was successfully loaded when the **FIPS** boot option was enabled. With this update, kernel self-integrity is improved by rejecting to load kernel modules which are not shipped by Red Hat when the **FIPS** boot option is enabled.

BZ#633964

A regression was discovered that caused kernel panic during the booting of any SGI UV100 and UV1000 system unless the **virtefi** command line option was passed to the kernel by GRUB. With this update, the need for the **virtefi** command line option is removed and the kernel will boots as expected without it.

BZ#633966

Previously, a Windows XP host experienced the stop error screen (i.e. the "Blue Screen Of Death" error) when booted with the CPU mode name. With this update, a Windows XP host no longer experiences the aforementioned error due to added KVM (Kernel-based Virtual Machine) support for the **MSR_EBC_FREQUENCY_ID** model specific register.

BZ#634973

Previously the cxgb3 (Chelsio Communications T3 10Gb Ethernet) adapter experienced parity errors. With this update, the parity errors are correctly detected and the cxgb3 adapter successfully recovers from them.

BZ#634984

Systems with an updated Video BIOS for the AMD RS880 would not properly boot with KMS (Kernel mode-setting) enabled. With this update, the Video BIOS boots successfully when KMS is enabled.

BZ#635951

The zfcpdump (kdump) kernel on IBM System z could not be debugged using the dump analysis tool **crash**, because the **vmlinux** file in the kernel-kdump-debuginfo RPM did not contain DWARF debug information. With this update, the ***CONFIG_DEBUG_KERNEL*** parameter is set to yes and the needed debug information is provided.

BZ#636116

Previously, **MADV_HUGEPAGE** was missing in the **include/asm-generic/mman-common.h** file which caused madvise to fail to utilize TPH. With this update, the madvise option was removed from **/sys/kernel/mm/redhat_transparent_hugepage/enabled** since **MADV_HUGEPAGE** was removed from the **madvise** system call.

BZ#637087

The kernel panicked when booting the kdump kernel on a **s390** system with an **initramfs** that contained an odd number of bytes. With this update, an **initramfs** with sufficient padding such that it contains an even number of bytes is generated, thus, the kernel no longer panics.

BZ#638973

Previously, in order to install Snapshot 13, boot parameter ***nomodeset xforcevesa*** had to be added to the kernel command line, otherwise, the screen turned black and prevented the installation. With this update, the aforementioned boot parameter no longer has to be specified and the installation works as expected.

BZ#639412

Previously, a write request may have merged with a discard request. This could have posed a potential risk for 3rd party drivers which could possibly issue a discard without waiting properly. With this update, discarding of write block I/O requests by preventing merges of discard and write requests in one block I/O has been introduced, thus, resolving the possible risks.

BZ#641258, BZ#644037

The **fork()** system call led to an **rmap** walk finding the parent **huge-pmd** twice instead of once, thus causing a discrepancy between the **mapcount** and **page_mapcount** check, which could have led to erratic page counts for subpages. This fix ensures that the **rmap** walk is accurate when a process is forked, thus resolving the issue.

BZ#641454

Running a **fsstress** test which issues various operations on a ext4 filesystem when **usrquota** is enabled, the following JBD (Journaling Block Device) error was output in **/var/log/messages**:

> JBD: Spotted dirty metadata buffer (dev = sda10, blocknr = 17635). There's a risk of filesystem corruption in case of system crash.

With this update, by always journaling the quota file modification in an ext4 file system the aforementioned message no longer appears in the logs.

BZ#641455

Previously, the destination MAC address validation was not checking for NPIV (N_Port ID Virtualization) addresses, which results in FCoE (Fibre Channel over Ethernet) frames being dropped. With this update, the destination MAC address check for FCoE frames has been modified so that multiple **N_port** IDs can be multiplexed on a single physical **N_port**.

BZ#641456

During an installation through Cisco NPV (N port virtualization) to Brocade, adding a LUN (Logical Unit Number) through **Add Advanced Target** did not work properly. This was caused by the faulty resending of FLOGI (Fabric Login) when a Fibre Channel switch in the NPV mode rejected requests with zero Destination ID. With this update, the LUN is seen and able to be selected for installation.

BZ#641457

Previously, timing issues could cause the FIP (FCoE Initialization Protocol) FLOGIs to timeout even if there were no problems. This caused the kernel to go into a non-FIP mode even though it should have been in the FIP mode. With this update, the timing issues no longer occur and the kernel no longer switches to the non-FIP mode when logging to the Fibre Channel Switch/Forwarder.

BZ#641458

Previously, the **vmstat** (virtual memory statistics) tool incorrectly reported the **disk I/O** as **swap-in** on ppc64 and other architectures that do not support the ***TRANSPARENT_HUGEPAGE*** configuration option in the kernel. With this update, the **vmstat** tool no longer reports incorrect statistics and works as expected.

BZ#641459

Previously, building under memory pressure with KSM (Kernel Shared Memory) caused KSM to collapse with an internal compiler error indicating an error in swapping. With this update, data corruption during swapping no longer occurs.

BZ#641460

Occasionally, the **anon_vma** variable could contain the value ***null*** in the **page_address_in_vma** function and cause kernel panic. With this update, kernel panic no longer occurs.

BZ#641483

Previously, the **/proc/maps** file which is read by LVM2 (Logical Volume Manager 2) contained inconsistencies caused by LVM2 incorrectly deciding which memory to **mlock** and **munlock**. With this update, LVM2 correctly decides between the **mlock** and **munlock** operations and no longer causes inconsistencies.

BZ#641907

Systems that have an Emulex FC controller (with SLI-3 based firmware) installed could return a kernel panic during installation. With this update, kernel panic no longer occurs during installation.

BZ#642043

This update fixes the slow memory leak in the i915 module in DRM (Direct Rendering Manager) and GEM (Graphics Execution Manager).

BZ#642045

Previously, a race condition in the TTM (Translation Table Maps) module of the DRM (Direct Rendering Manager) between the object destruction thread and object eviction could result in a major loss of large objects reference counts. Consequently, this caused a major amount of memory leak. With this update, the race condition no longer occurs and any memory leaks are prevented.

BZ#642679

Previously, an operation such as **madvise(MADV_MERGEABLE)** may have split VMAs (Virtual Memory Area) without checking if any huge page had to be split into regular pages, leading to huge pages to be still mapped in VMA ranges that would not be large enough to fit huge pages. With this update, huge pages are checked whether they have been split when any VMA is being truncated.

BZ#642680

Previously, accounting of reclaimable inodes did not work correctly. When an inode was reclaimed it was only deleted from the per-AG (per Allocation Group) tree. Neither the counter was decreased, nor was the parent tree's AG entry untagged properly. This caused the system to hang indefinitely. With this update, the accounting of reclaimable inodes works properly and the system remains responsive.

BZ#644038

A race condition occurred when Xen was presented with an inconsistent page type resulting in the crash of the kernel. With this update, the race condition is prevented and kernel crashes no longer occur.

BZ#644636

Previously, Red Hat Enterprise Linux 6 enabled the ***CONFIG_IMA*** option in the kernel. This caused the kernel to track all inodes in the system in a radix tree, leading to a huge waste of memory. With this update, an optimized version of a tree (rbtree) is used and memory is no longer wasted.

BZ#644926

Previously, calling the **elevator_change** function immediately after the **blk_init_queue** function resulted in a null pointer dereference. With this update, the null pointer dereference no longer occurs.

BZ#646994

When booting the latest Red Hat Enterprise Linux 6 kernel (-78.el6), the system hanged shortly after the booting. Access to the file system died and the console started outputting soft lockup messages from the TTM code. With this update, the aforementioned behavior no longer occurs and the system boots as expected.

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.

B.38.2. RHSA-2011:0007 – Important: kernel security and bug fix update

IMPORTANT

This update has already been released as the security errata RHSA-2011:0007

Updated kernel packages that fix multiple security issues and several 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. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:
* Buffer overflow in **eCryptfs**. When **/dev/ecryptfs** has world writable permissions (which it does not, by default, on Red Hat Enterprise Linux 6), a local, unprivileged user could use this flaw to cause a denial of service or possibly escalate their privileges. (CVE-2010-2492, Important)

* Integer overflow in the **RDS** protocol implementation could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2010-3865, Important)

* Missing boundary checks in the **PPP** over **L2TP** sockets implementation could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2010-4160, Important)

* NULL pointer dereference in the **igb** driver. If both Single Root I/O Virtualization (SR-IOV) and promiscuous mode were enabled on an interface using **igb**, it could result in a denial of service when a tagged VLAN packet is received on that interface. (CVE-2010-4263, Important)

* Missing initialization flaw in the **XFS** file system implementation, and in the network traffic policing implementation, could allow a local, unprivileged user to cause an information leak. (CVE-2010-3078, CVE-2010-3477, Moderate)

* NULL pointer dereference in the Open Sound System compatible sequencer driver could allow a local, unprivileged user with access to **/dev/sequencer** to cause a denial of service. **/dev/sequencer** is only accessible to root and users in the audio group by default. (CVE-2010-3080, Moderate)

* Flaw in the ethtool IOCTL handler could allow a local user to cause an information leak. (CVE-2010-3861, Moderate)

* Flaw in **bcm_connect()** in the Controller Area Network (CAN) Broadcast Manager. On 64-bit systems, writing the socket address may overflow the ***procname*** character array. (CVE-2010-3874, Moderate)

* Flaw in the module for monitoring the sockets of **INET** transport protocols could allow a local, unprivileged user to cause a denial of service. (CVE-2010-3880, Moderate)

* Missing boundary checks in the block layer implementation could allow a local, unprivileged user to cause a denial of service. (CVE-2010-4162, CVE-2010-4163, CVE-2010-4668, Moderate)

* NULL pointer dereference in the Bluetooth **HCI UART** driver could allow a local, unprivileged user to cause a denial of service. (CVE-2010-4242, Moderate)

* Flaw in the Linux kernel CPU time clocks implementation for the POSIX clock interface could allow a local, unprivileged user to cause a denial of service. (CVE-2010-4248, Moderate)

* Flaw in the garbage collector for **AF_UNIX** sockets could allow a local, unprivileged user to trigger a denial of service. (CVE-2010-4249, Moderate)

* Missing upper bound integer check in the AIO implementation could allow a local, unprivileged user to cause an information leak. (CVE-2010-3067, Low)

* Missing initialization flaws could lead to information leaks. (CVE-2010-3298, CVE-2010-3876, CVE-2010-4072, CVE-2010-4073, CVE-2010-4074, CVE-2010-4075, CVE-2010-4077, CVE-2010-4079, CVE-2010-4080, CVE-2010-4081, CVE-2010-4082, CVE-2010-4083, CVE-2010-4158, Low)

* Missing initialization flaw in KVM could allow a privileged host user with access to **/dev/kvm** to cause an information leak. (CVE-2010-4525, Low)

Red Hat would like to thank Andre Osterhues for reporting CVE-2010-2492; Thomas Pollet for reporting CVE-2010-3865; Dan Rosenberg for reporting CVE-2010-4160, CVE-2010-3078, CVE-2010-3874, CVE-2010-4162, CVE-2010-4163, CVE-2010-3298, CVE-2010-4073, CVE-2010-4074, CVE-2010-4075, CVE-2010-4077, CVE-2010-4079, CVE-2010-4080, CVE-2010-4081, CVE-2010-4082, CVE-2010-4083, and CVE-2010-4158; Kosuke Tatsukawa for reporting CVE-2010-4263; Tavis Ormandy for reporting CVE-2010-3080 and CVE-2010-3067; Kees Cook for reporting CVE-2010-3861 and CVE-2010-4072; Nelson Elhage for reporting CVE-2010-3880; Alan Cox for reporting CVE-2010-4242; Vegard Nossum for reporting CVE-2010-4249; Vasiliy Kulikov for reporting CVE-2010-3876; and Stephan Mueller of atsec information security for reporting CVE-2010-4525.

Bug fixes:

BZ#655122

When building kernel modules against the full Red Hat Enterprise Linux 6 source tree (instead of just kernel-devel), modules would be signed by a locally generated key. However, Red Hat Enterprise Linux 6 refused to load modules created in this way as it did not recognize the key. This update disables module signing while building out-of-tree modules, thus, in the aforementioned case, kernel module loading works as expected.

BZ#643815

With this update, the upper limit of the ***log_mtts_per_seg*** variable was increased from five to seven, increasing the amount of memory that can be registered. As a result, the Mellanox driver (**mlx4**) can now use up to 64 GB of physical memory for RDMA (remote direct memory access). This provides better scalability for example when using the Mellanox adapter in NFS/RDMA, or on machines with a lot of physical memory.

BZ#648408

Due to a mix-up between ***FMODE_*** and ***O_*** flags, an **NFSv4** client could get a ***WRITE*** lock on a file that another **NFSv4** client already had a ***READ*** lock on. As a result, data could be corrupted. With this update, ***FMODE_*** and ***O_*** flags are properly handled and getting a ***WRITE*** lock fails in the aforementioned case.

BZ#649436

Booting Red Hat Enterprise Linux 6 debug kernel on a system with the Dell PowerEdge RAID Controller H700 adapter caused the **megaraid_sas** driver to reset the controller multiple times leading to a faulty controller state. On rebooting the system, the faulty controller state could cause the firmware to detect an incorrect memory condition. This could be especially confusing since the message could be a faulty DIMM (Dual In-line Memory Module) condition prompting the administrator to replace the DIMMs. This occurred due to a leak in the ***mfi_sgl*** dma'ed frame when the firmware supported IEEE frames. The ***mfi_sgl*** would draw memory from the slab cache and any use of freed memory would result in incorrect pages being read in the ISR (Interrupt Service Routine). This caused the controller resets and the ensuing DIMM error condition. This update fixes the leak in ***mfi_sgl*** when the firmware supports IEEE frames. Faulty controller states and faulty DIMM conditions no longer occur.

BZ#653900

Running VDSM and performing an **lvextend** operation during an intensive Virtual Guest power up caused this operation to fail. Since **lvextend** was blocked, all components became non-responsive: **vgs** and **lvs** commands froze the session, Virtual Guests became *Paused* or *Not Responding*. This was caused due to a faulty use of a lock. With this update, performing an **lvextend** operation works as expected.

BZ#651996

Due to a faulty memory allocator, on Non-Uniform Memory Architecture (NUMA) platforms, an OOM (Out Of Memory) condition would occur when a user changed a cpuset's **/etc/dev/mems** file (list of memory nodes in that cpuset) even though the specified node had enough free memory. With this update, the memory allocator no longer causes an OOM condition when a node has enough free memory.

BZ#653340

When using a VIRT-IO (Virtual Input/Output) NIC (Network Interface Controller), its state was reported as *unknown* instead of its real state (*up* or *down*). This was due to the fact that the device could not report the state status. With this update, when a device is not capable of reporting the current state, it is assumed the state is *up* or the state is read from the config file.

BZ#658879

A previously released patch fixed the external module compiling when using the full source tree, however, it was discovered it resulted in breaking the build in the kernel-devel only case. With this update, the patch has been fixed to avoid any external module compiling errors.

BZ#647391

Running certain workload tests on a NUMA (Non-Uniform Memory Architecture) system could cause kernel panic at ***mm/migrate.c:113***. This was due to a false positive BUG_ON. With this update, the false positive BUG_ON has been removed.

BZ#659611

Updated partner qualification injecting target faults uncovered a flaw where the Emulex **lpfc** driver would incorrectly panic due to a null **pnode** dereference. This update addresses the issue and was tested successfully under the same test conditions without the panic occurring.

BZ#660589

Updated partner qualification injecting controller faults uncovered a flaw where the Emulex **lpfc** driver panicked during error handling. With this update, kernel panic no longer occurs.

BZ#660244

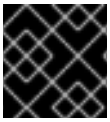
Updated partner qualification injecting controller faults uncovered a flaw where Fibre Channel ports would go offline while testing with Emulex LPFC controllers due to a faulty LPFC heartbeat functionality. This update changes the default behavior of the LPFC heartbeat to ***off***.

BZ#660591

When configuring an SIT (Simple Internet Transition) tunnel while a remote address is configured, kernel panic occurred, caused by an execution of a **NULL *header_ops*** pointer in the **neigh_update_hhs()** function. With this update, a check is introduced that makes sure the ***header_ops*** pointer is not of the value **NULL**, thus, kernel panic no longer occurs.

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.

B.38.3. RHSA-2011:0283 – Moderate: kernel security, bug fix and enhancement update



IMPORTANT

This update has already been released as the security errata RHSA-2011:0283

Updated kernel packages that resolve several security issues, fix various bugs and add 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 after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes

* A divide-by-zero flaw was found in the **tcp_select_initial_window()** function in the Linux kernel's **TCP/IP** protocol suite implementation. A local, unprivileged user could use this flaw to trigger a denial of service by calling **setsockopt()** with certain options. (CVE-2010-4165, Moderate)

* A use-after-free flaw in the **mprotect()** system call in the Linux kernel could allow a local, unprivileged user to cause a local denial of service. (CVE-2010-4169, Moderate)

* A flaw was found in the Linux kernel **execve()** system call implementation. A local, unprivileged user could cause large amounts of memory to be allocated but not visible to the OOM (Out of Memory) killer, triggering a denial of service. (CVE-2010-4243, Moderate)

Red Hat would like to thank Steve Chen for reporting CVE-2010-4165, and Brad Spengler for reporting CVE-2010-4243.

Bug fixes

BZ#652720

Prior to this update, a guest could use the **poll()** function to find out whether the host-side connection was open or closed. However, with a ***SIGIO*** signal, this can be done asynchronously, without having to explicitly poll each port. With this update, a ***SIGIO*** signal is sent for any host connect/disconnect events. Once the ***SIGIO*** signal is received, the open/close status of **virtio-serial** ports can be obtained using the **poll()** system call.

BZ#658854

A Red Hat Enterprise Linux 6.0 host (with root on a local disk) with **dm-multipath** configured on multiple LUNs (Logical Unit Number) hit kernel panic (at **scsi_error_handler**) with target controller faults during an I/O operation on the **dm-multipath** devices. This was caused by **multipath** using the **blk_abort_queue()** function to allow lower latency path deactivation. The call to ***blk_abort_queue*** proved to be unsafe due to a race (between ***blk_abort_queue*** and ***scsi_request_fn***). With this update, the race has been resolved and kernel panic no longer occurs on Red Hat Enterprise Linux 6.0 hosts.

BZ#658891

Prior to this update, running context-switch intensive workloads on KVM guests resulted in a large number of exits (***kvm_exit***) due to control register (CR) accesses by the guest, thus, resulting in poor performance. This update includes a number of optimizations which allow the guest not to exit to the hypervisor in the aforementioned case and improve the overall performance.

BZ#659610

Handling ALUA (Asymmetric Logical Unit Access) *transitioning* states did not work properly due to a

Handling ALUA (Asymmetric Logical Unit Access) *transitioning* states did not work properly due to a faulty **SCSI** (Small Computer System Interface) **ALUA** handler. With this update, optimized state transitioning prevents the aforementioned behavior.

BZ#660590

Prior to this update, when using Red Hat Enterprise Linux 6 with a **qla4xxx** driver and **FC** (Fibre Channel) drivers using the **fc** class, a device might have been put in the *offline* state due to a transport problem. Once the transport problem was resolved, the device was not usable until a user manually corrected the state. This update enables the transition from the *offline* state to the *running* state, thus, fixing the problem.

BZ#661667

The **zfcpdump** tool was not able to mount **ext4** file systems. Because **ext4** is the default file system on Red Hat Enterprise Linux 6, with this update, **ext4** file system support was added for the **zfcpdump** tool.

BZ#661725

The **zfcpdump** tool was not able to mount **ext2** file systems. With this update, **ext2** file system support was added for the **zfcpdump** tool.

BZ#661730

The *lock reclaim* operation on a Red Hat Enterprise Linux 6 **NFSv4** client did not work properly when, after a server reboot, an I/O operation which resulted in a ***STALE_STATEID*** response was performed before the ***RENEW*** call was sent to the server. This behavior was caused due to the improper use of the state flags. While investigating this bug, a different bug was discovered in the *state recovery* operation which resulted in a reclaim thread looping in the **nfs4_reclaim_open_state()** function. With this update, both operations have been fixed and work as expected.

BZ#661731

Prior to this update, the **execve** utility exhibited the following flaw. When an argument and any environment data were copied from an old task's user stack to the user stack of a newly-execve'd task, the kernel would not allow the process to be interrupted or rescheduled. Therefore, when the argument or environment string data was (abnormally) large, there was no "interactivity" with the process while the **execve()** function was transferring the data. With this update, fatal signals (like **CTRL**+**c**) can now be received and handled and a process is allowed to yield to higher priority processes during the data transfer.

BZ#661732

The *memory* cgroup controller has its own Out of Memory routine (OOM killer) and kills a process at an OOM event. However, a race condition could cause the **pagefault_out_of_memory** function to be called after the *memory* cgroup's OOM. This invoked the generic OOM killer and a ***panic_on_oom*** could occur. With this update, only the *memory* cgroup's OOM killer is invoked and used to kill a process should an OOM occur.

BZ#661737

In some cases, under a small system load involve some I/O operation, processes started to lock up in the **D** state (that is, became unresponsive). The system load could in some cases climb steadily. This was due to the way the event channel IRQ (Interrupt Request) was set up. Xen events behave like edge-triggered IRQs, however, the kernel was setting them up as level-triggered IRQs. As a result, any action using Xen event channels could lock up a process in the **D** state. With this update, the handling has been changed from edge-triggered IRQs to level-triggered IRQs and process no longer lock up in the **D** state.

BZ#662049

When an **scsi** command timed out and the **fcoe**/**libfc** driver aborted the command, a race could occur during the clean-up of the command which could result in kernel panic. With this update, the locking mechanism in the clean-up and abort paths was modified, thus, fixing the aforementioned issue.

BZ#662050

The lack of synchronization between the clearing of the ***QUEUE_FLAG_CLUSTER*** flag and the setting of the ***no_cluster*** flag in the ***queue_limits*** variable caused corruption of data. Note that this issue only occurred on hardware that did not support segment merging (that is, clustering). With this update, the synchronization between the aforementioned flags works as expected, thus, corruption of data no longer occurs.

BZ#662721

The **virtio-console** device did not handle the *hot-unplug* operation properly. As a result, **virtio-console** could access the memory outside the driver's memory area and cause kernel panic on the guest. With this update, multiple fixes to the **virtio-console** device resolved this issue and the *hot-unplug* operation works as expected.

BZ#662921

Prior to this update, running the **hwclock --systohc** command could halt a running system. This was due to the interrupt transactions being looped back from a local IOH (Input/Output Hub), through the IOH to a local CPU (erroneously), which caused a conflict with I/O port operations and other transactions. With this update, the conflicts are avoided and the system continues to run after executing the **hwclock --systohc** command.

BZ#666797

An I/O operation could fast fail when using Device-Mapper Multipathing (**dm-multipath**) if the I/O operation could be retried by the **scsi** layer. This prevented the *multipath* layer from starting its error recovery procedure and resulted in unnecessary log messages in the appropriate log files. This update includes a number of optimizations that resolve the aforementioned issue.

BZ#670421

Outgoing packets were not fragmented after receiving the icmpv6 pkt-too-big message when using the **IPSecv6** tunnel mode. This was due to the lack of **IPv6** fragmentation support over an **IPsec** tunnel. With this update, **IPv6** fragmentation is fully supported and works as expected when using the **IPSecv6** tunnel mode.

BZ#671342

Bonding, when operating in the **ARP** monitoring mode, made erroneous assumptions regarding the ownership of **ARP** frames when it received them for processing. Specifically, it was assumed that the bonding driver code was the only execution context which had access to the **ARP** frames network buffer data. As a result, an operation was attempted on the said buffer (specifically, to modify the size of the data buffer) which was forbidden by the kernel when a buffer was shared among several execution contexts. The result of such an operation on a shared buffer could lead to data corruption. Consequently, trying to prevent the corruption, the kernel panicked. This *shared state* in the network buffer could be forced to occur, for example, when running the **tcpdump** utility to monitor traffic on the bonding interface. Every buffer the bond interface received would be shared between the driver and the **tcpdump** process, thus, resulting in the aforementioned kernel panic. With this update, for the particular affected path in the bonding driver, each inbound frame is checked whether it is in the *shared state*. In case a buffer is shared, a private copy is made for exclusive use by the bonding driver, thus, preventing the kernel panic.

BZ#673978

For a device that used a Target Portal Group (TPG) ID which occupied the full 2 bytes in the RTPG (Report Target Port Groups) response (with either byte exceeding the maximum value that may be stored in a signed char), the kernel's calculated TPG ID would never match the ***group_id*** that it should. As a result, this signed char overflow also caused the ALUA handler to incorrectly identify the Asymmetric Access State (AAS) of the specified device as well as incorrectly interpret the supported AAS of the target. With this update, the aforementioned issue has been addressed and no longer occurs.

Enhancements

BZ#674002

The **ixgbe** driver has been updated to address various FCoE (Fibre Channel over Ethernet) issues related to Direct Data Placement (FCoE DDP).

BZ#664398

The **qla2xxx** driver for QLogic Fibre Channel Host Bus Adapters (HBAs) has been updated to upstream version 8.03.05.01.06.1-k0, which provides a number of bug fixes and enhancements over the previous version.

Users should upgrade to these updated packages, which contain backported patches to correct these issues, fix these bugs, and add these enhancements. The system must be rebooted for this update to take effect.

B.38.4. RHSA-2011:0329 – Important: kernel security update

Updated kernel 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.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

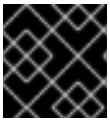
CVE-2011-0714, Important

A use-after-free flaw was found in the Linux kernel's RPC server sockets implementation. A remote attacker could use this flaw to trigger a denial of service by sending a corrupted packet to a target system.

Red Hat would like to thank Adam Prince for reporting this issue.

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.

B.38.5. RHSA-2011:0421 – Important: kernel security and bug fix update



IMPORTANT

This update has already been released as the security errata RHSA-2011:0421

Updated kernel packages that resolve several security issues and fix 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. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes
* A flaw was found in the **sctp_icmp_proto_unreachable()** function in the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation. A remote attacker could use this flaw to cause a denial of service. (CVE-2010-4526, Important)

* A missing boundary check was found in the **dvb_ca_ioctl()** function in the Linux kernel's **av7110** module. On systems that use old DVB cards that require the **av7110** module, a local, unprivileged user could use this flaw to cause a denial of service or escalate their privileges. (CVE-2011-0521, Important)

* A race condition was found in the way the Linux kernel's InfiniBand implementation set up new connections. This could allow a remote user to cause a denial of service. (CVE-2011-0695, Important)

* A heap overflow flaw in the **iowarrior_write()** function could allow a user with access to an IO-Warrior USB device, that supports more than 8 bytes per report, to cause a denial of service or escalate their privileges. (CVE-2010-4656, Moderate)

* A flaw was found in the way the Linux Ethernet bridge implementation handled certain IGMP (Internet Group Management Protocol) packets. A local, unprivileged user on a system that has a network interface in an Ethernet bridge could use this flaw to crash that system. (CVE-2011-0716, Moderate)

* A NULL pointer dereference flaw was found in the Generic Receive Offload (GRO) functionality in the Linux kernel's networking implementation. If both GRO and promiscuous mode were enabled on an interface in a virtual LAN (VLAN), it could result in a denial of service when a malformed VLAN frame is received on that interface. (CVE-2011-1478, Moderate)

* A missing initialization flaw in the Linux kernel could lead to an information leak. (CVE-2010-3296, Low)

* A missing security check in the Linux kernel's implementation of the install_special_mapping routine could allow a local, unprivileged user to bypass the **mmap_min_addr** protection mechanism. (CVE-2010-4346, Low)

* A logic error in the **orinoco_ioctl_set_auth()** function in the Linux kernel's ORiNOCO wireless extensions support implementation could render TKIP countermeasures ineffective when it is enabled, as it enabled the card instead of shutting it down. (CVE-2010-4648, Low)

* A missing initialization flaw was found in the **ethtool_get_regs()** function in the Linux kernel's ethtool IOCTL handler. A local user who has the ***CAP_NET_ADMIN*** capability could use this flaw to cause an information leak. (CVE-2010-4655, Low)

* An information leak was found in the Linux kernel's **task_show_regs()** implementation. On IBM S/390 systems, a local, unprivileged user could use this flaw to read /**proc**/***<PID>***/**status** files, allowing them to discover the CPU register values of processes. (CVE-2011-0710, Low)

Red Hat would like to thank Jens Kuehnel for reporting CVE-2011-0695; Kees Cook for reporting CVE-2010-4656 and CVE-2010-4655; Dan Rosenberg for reporting CVE-2010-3296; and Tavis Ormandy for reporting CVE-2010-4346.

Bug fixes

BZ#678484

The **bnx2i** driver could cause a system crash on IBM POWER7 systems. The driver's page tables were not set up properly on Big Endian machines, causing extended error handling (EEH) errors on PowerPC machines. With this update, the page tables are properly set up and a system crash no longer occurs in the aforementioned case.

BZ#678485

On platforms using an Intel 7500 or an Intel 5500 chipset (or their derivatives), occasionally, a VT-d specification defined error occurred in the **kdump** kernel (the second kernel). As a result of the VT-d error, on some platforms, an SMI (System Management Interrupt) was issued and the system became unresponsive. With this update, a VT-d error is properly handled so that an SMI is no longer issued, and the system no longer hangs.

BZ#678558

Using a **virtio** serial port from an application, filling it until the **write** command returns ***-EAGAIN*** and then executing a **select** command for the **write** command, caused the **select** command to not return any values when using the **virtio** serial port in a *non-blocking* mode. When used in *blocking* mode, the **write** command waited until the host indicated it had used up the buffers. This was due to the fact that the poll operation waited for the ***port->waitqueue*** pointer; however, nothing woke the ***waitqueue*** when there was room again in the queue. With this update, the queue is woken via host notifications so that buffers consumed by the host can be reclaimed, the queue freed, and the application **write** operations may proceed again.

BZ#678559

Prior to this update, user space could submit (using the **write()** operation) a buffer with zero length to be written to the host, causing the qemu hypervisor instance running on that host to crash. This was caused by the **write()** operation triggering a **virtqueue** event on the host, causing a **NULL** buffer to be accessed. With this update, user space is no longer allowed to submit zero-sized buffers and the aforementioned crash no longer occur.

BZ#678561

Applications and agents using **virtio** serial ports would block messages even though there were messages queued up and ready to be read in the **virtqueue**. This was due to **virtio_console**'s poll function checking whether a port was **NULL** to determine if a read operation would result in a block of the port. However, in some cases, a port can be **NULL** even though there are buffers left in the **virtqueue** to be read. This update introduces a more sophisticated method of checking whether a port contains any data; thus, preventing queued up messages from being incorrectly blocked.

BZ#678562

If a host was slow in reading data or did not read data at all, blocking **write()** calls not only blocked the program that called the **write()** call but also the entire guest. This was caused by the **write()** calls waiting until an acknowledgment that the data consumed was received from the host. With this update, **write()** calls no longer wait for such acknowledgment: control is immediately returned to the user space application. This ensures that even if the host is busy processing other data or is not consuming data at all, the guest is not blocked.

BZ#678996

An implementation of the SHA (Secure Hash Algorithm) hashing algorithm for the IBM System z architecture did not produce correct hashes and could potentially cause memory corruption due to broken partial block handling. A partial block could break when it was followed by an update which

filled it with leftover bytes. Instead of storing the new leftover bytes at the start of the buffer, they were stored immediately after the previous partial block. With this update, the index pointer is reset, thus resolving the aforementioned partial block handling issue.

BZ#680080

Prior to this update, performing live migration back and forth during guest installation with network adapters based on the 8168c chipset or the 8111c chipset triggered an ***rtl8169_interrupt*** hang due to a RxFIFO overflow. With this update, infinite loops in the IRQ (Interrupt Request) handler caused by RxFIFO overflows are prevented and the aforementioned hang no longer occurs.

BZ#683442

Reading the **/proc/vmcore** file was previously significantly slower on a Red Hat Enterprise Linux 6 system when compared to a Red Hat Enterprise Linux 5 system. This update enables caching of memory accesses; reading of the **/proc/vmcore** file is now noticeably faster.

BZ#683445

Reading the **/proc/vmcore** file on a Red Hat Enterprise Linux 6 system was not optimal because it did not always take advantage of reading through the cached memory. With this update, access to the **/dev/oldmem** device in the **/proc/vmcore** file is cached, resulting in faster copying to user space.

BZ#683781

Migrating a guest could have resulted in dirty values for the guest being retained in memory, which could have caused both the guest and qemu to crash. The trigger for this was memory pages being both write-protected and dirty simultaneously. With this update, memory pages in the current bitmap are either dirty or write-protected when migrating a guest, with the result that neither qemu nor guest operating systems crash following a migration.

BZ#683783

While not mandated by any specification, Linux systems rely on NMIs (**N**on-**m**askable **I**nterrupts) being blocked by an IF-enabling (**I**nterrupt **F**lag) STI instruction (an x86 instruction that enables interrupts; **S**e**t** **I**nterrupts); this is also the common behavior of all known hardware. Prior to this update, kernel panic could occur on guests using NMIs extensively (for example, a Linux system with the ***nmi_watchdog*** kernel parameter enabled). With this update, an NMI is disallowed when interrupts are blocked by an STI. This is done by checking for the condition and requesting an interrupt window exit if it occurs. As a result, kernel panic no longer occurs.

BZ#683812

Under certain circumstances, a kernel thread that handles incoming messages from a server could unexpectedly exit by itself. As a result, the kernel thread would free some data structures which could then be referenced by another data structure, resulting in a kernel panic. With this update, kernel threads no longer unexpectedly exit; thus, kernel panic no longer occurs in the aforementioned case.

BZ#683814

Operating in the FIP (FCoE Initialization Protocol) mode and performing operations that bring up ports could cause the **fcoe.ko** and **fnic.ko** modules to not be able to re-login when a port was brought back up. This was due to a bug in the FCoE (Fiber Channel over Ethernet) layer causing improper handling of FCoE LOGO frames while in the FIP mode. With this update, FCoE LOGO frames are properly handled when in the FIP mode and the **fcoe.ko** and **fnic.ko** modules no longer fail to re-login.

BZ#683815

If a CPU is set offline, the ***nohz_load_balancer*** CPU is updated. However, under certain circumstances, the ***nohz_load_balancer*** CPU would not be updated, causing the offlined CPU to be enqueued with various timers which never expired. As a result, the system could become unresponsive. With this update, the ***nohz_load_balancer*** CPU is always updated; systems no longer become unresponsive.

BZ#683822

The kernel syslog contains debugging information that is often useful during exploitation of other vulnerabilities such as kernel heap addresses. With this update, a new **CONFIG_SECURITY_DMESG_RESTRICT** option has been added to config-generic-rhel which prevents unprivileged users from reading the kernel syslog. This option is by default turned off (***0***), which means no restrictions.

BZ#684129

Prior to this update, the default VF (Virtual Function) configuration was not restrictive enough. With this update, VFs only accept broadcast and multicast frames and do not accept frames from the unicast MAC address table. Restrictions are now also properly set on what can be received when the device is put in promiscuous mode. A hardware limitation was also discovered that prevented the system from properly receiving certain FCoE (Fibre Channel over Ethernet) protocol frames of a specific size. A buffer management change now allows these frames to be properly received.

BZ#684266

PowerPC systems having more than 1 TB of RAM could randomly crash or become unresponsive due to an incorrect setup of the Segment Lookaside Buffer (SLB) entry for the kernel stack. With this update, the SLB entry is properly set up.

BZ#684267

On IBM System z systems, user space programs could access the **/dev/mem** file (which contains an image of main memory), where an accidental memory (write) access could potentially be harmful. To restrict access to memory from user space through the **/dev/mem** file, the **CONFIG_STRICT_DEVMEM** configuration option has been enabled for the default kernel. The kdump and debug kernels have this option switched off by default.

BZ#684268

Intensive usage of resources on a guest lead to a failure of networking on that guest: packets could no longer be received. The failure occurred when a DMA (Direct Memory Access) ring was consumed before NAPI (New API; an interface for networking devices which makes use of interrupt mitigation techniques) was enabled which resulted in a failure to receive the next interrupt request. The regular interrupt handler was not affected in this situation (because it can process packets in-place), however, the OOM (Out Of Memory) handler did not detect the aforementioned situation and caused networking to fail. With this update, NAPI is subsequently scheduled for each **napi_enable** operation; thus, networking no longer fails under the aforementioned circumstances.

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.

B.38.6. RHSA-2011:0498 – Important: kernel security, bug fix and enhancement update

IMPORTANT

This update has already been released as the security errata RHSA-2011:0498

Updated kernel packages that resolve several security issues, fix various bugs and add an 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. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes
* An integer overflow flaw in **ib_uverbs_poll_cq()** could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2010-4649, Important)

* An integer signedness flaw in **drm_modeset_ctl()** could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2011-1013, Important)

* The Radeon GPU drivers in the Linux kernel were missing sanity checks for the Anti Aliasing (AA) resolve register values which could allow a local, unprivileged user to cause a denial of service or escalate their privileges on systems using a graphics card from the ATI Radeon R300, R400, or R500 family of cards. (CVE-2011-1016, Important)

* A flaw in **dccp_rcv_state_process()** could allow a remote attacker to cause a denial of service, even when the socket was already closed. (CVE-2011-1093, Important)

* A flaw in the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation could allow a remote attacker to cause a denial of service if the sysctl ***net.sctp.addip_enable*** and ***auth_enable*** variables were turned on (they are off by default). (CVE-2011-1573, Important)

* A memory leak in the **inotify_init()** system call. In some cases, it could leak a group, which could allow a local, unprivileged user to eventually cause a denial of service. (CVE-2010-4250, Moderate)

* A missing validation of a null-terminated string data structure element in **bnep_sock_ioctl()** could allow a local user to cause an information leak or a denial of service. (CVE-2011-1079, Moderate)

* An information leak in **bcm_connect()** in the Controller Area Network (CAN) Broadcast Manager implementation could allow a local, unprivileged user to leak kernel mode addresses in **/proc/net/can-bcm**. (CVE-2010-4565, Low)

* A flaw was found in the Linux kernel's Integrity Measurement Architecture (IMA) implementation. When SELinux was disabled, adding an IMA rule which was supposed to be processed by SELinux would cause **ima_match_rules()** to always succeed, ignoring any remaining rules. (CVE-2011-0006, Low)

* A missing initialization flaw in the XFS file system implementation could lead to an information leak. (CVE-2011-0711, Low)

* Buffer overflow flaws in **snd_usb_caiaq_audio_init()** and **snd_usb_caiaq_midi_init()** could allow a local, unprivileged user with access to a Native Instruments USB audio device to cause a denial of service or escalate their privileges. (CVE-2011-0712, Low)

* The start_code and end_code values in **/proc/*<PID>*/stat** were not protected. In certain scenarios, this flaw could be used to defeat Address Space Layout Randomization (ASLR). (CVE-2011-0726, Low)

* A flaw in **dev_load()** could allow a local user who has the ***CAP_NET_ADMIN*** capability to load arbitrary modules from **/lib/modules/**, instead of only netdev modules. (CVE-2011-1019, Low)

* A flaw in **ib_uverbs_poll_cq()** could allow a local, unprivileged user to cause an information leak. (CVE-2011-1044, Low)

* A missing validation of a null-terminated string data structure element in **do_replace()** could allow a local user who has the ***CAP_NET_ADMIN*** capability to cause an information leak. (CVE-2011-1080, Low)

Red Hat would like to thank Vegard Nossum for reporting CVE-2010-4250; Vasiliy Kulikov for reporting CVE-2011-1079, CVE-2011-1019, and CVE-2011-1080; Dan Rosenberg for reporting CVE-2010-4565 and CVE-2011-0711; Rafael Dominguez Vega for reporting CVE-2011-0712; and Kees Cook for reporting CVE-2011-0726.

Bug fixes

BZ#659572

A flaw was found in the Linux kernel where, if used in conjunction with another flaw that can result in a kernel Oops, could possibly lead to privilege escalation. It does not affect Red Hat Enterprise Linux 6 as the **sysctl *panic_on_oops*** variable is turned on by default. However, as a preventive measure if the variable is turned off by an administrator, this update addresses the issue. Red Hat would like to thank Nelson Elhage for reporting this vulnerability.

BZ#694073

Under some circumstances, faulty logic in the system BIOS could report that ASPM (Active State Power Management) was not supported on the system, but leave ASPM enabled on a device. This could lead to AER (Advanced Error Reporting) errors that the kernel was unable to handle. With this update, the kernel proactively disables ASPM on devices when the BIOS reports that ASPM is not supported, safely eliminating the aforementioned issues.

BZ#696487

Prior to this update, adding a bond over a bridge inside a virtual guest caused the kernel to crash due to a NULL dereference. This update improves the tests for the presence of VLANs configured above bonding (additionally, this update fixes a regression introduced by the patch for BZ#633571) . The new logic determines whether a registration has occurred, instead of testing that the internal ***vlan_list*** of a bond is empty. Previously, the system panicked and crashed when ***vlan_list*** was not empty, but the ***vlgrp*** pointer was still **NULL**.

BZ#698109

During light or no network traffic, the active-backup interface bond using ARP monitoring with validation could go down and return due to an overflow or underflow of system timer interrupt ticks (jiffies). With this update, the jiffies calculation issues have been fixed and a bond interface works as expected.

BZ#691777

In certain network setups (specifically, using VLAN on certain NICs where packets are sent through the VLAN GRO rx path), sending packets from an active ethernet port to another inactive ethernet port could affect the network's bridge and cause the bridge to acquire a wrong bridge port. This resulted in all packets not being passed along in the network. With this update, the underlying source code has been modified to address this issue, and network traffic works as expected.

BZ#698114, BZ#696889

Deleting a **SCSI** (Small Computer System Interface) device attached to a device handler caused applications running in user space, which were performing I/O operations on that device, to become unresponsive. This was due to the fact that the **SCSI** device handler's activation did not propagate the **SCSI** device deletion via an error code and a callback to the Device-Mapper Multipath. With this update, deletion of an **SCSI** device attached to a device handler is properly handled and no longer causes certain applications to become unresponsive.

BZ#683440

Systems Management Applications using the libsmbios package could become unresponsive on Dell PowerEdge servers (specifically, Dell PowerEdge 2970 and Dell PowerEdge SC1435). The **dcdbas** driver can perform an I/O write operation which causes an SMI (System Management Interrupt) to occur. However, the SMI handler processed the SMI well after the **outb** function was processed, which caused random failures resulting in the aforementioned hang. With this update, the underlying source code has been modified to address this issue, and systems management applications using the libsmbios package no longer become unresponsive.

BZ#670850

Invoking an EFI (Extensible Firmware Interface) call caused a restart or a failure to boot to occur on a system with more than 512GB of memory because the EFI page tables did not map the whole kernel space. EFI page tables used only one PGD (Page Global Directory) entry to map the kernel space; thus, virtual addresses higher than ***PAGE_OFFSET*** + 512GB could not be accessed. With this update, EFI page tables map the whole kernel space.

BZ#683820

Enabling the Header Splitting mode on all Intel 82599 10 Gigabit Ethernet hardware could lead to unpredictable behavior. With this update, the Header Splitting mode is never enabled on the aforementioned hardware.

BZ#670114

The **ixgbe** driver has been upgraded to upstream version 3.0.12, which provides a number of bug fixes and enhancements over the previous version.

BZ#670110

If an Intel 82598 10 Gigabit Ethernet Controller was configured in a way that caused peer-to-peer traffic to be sent to the Intel X58 I/O hub (IOH), a PCIe credit starvation problem occurred. As a result, the system would hang. With this update, the system continues to work and does not hang.

BZ#683817

The ALSA HDA audio driver has been updated to improve support for new chipsets and HDA audio codecs.

BZ#689341

A buffer overflow flaw was found in the Linux kernel's Cluster IP hashmark target implementation. A local, unprivileged user could trigger this flaw and cause a local denial of service by editing files in the **/proc/net/ipt_CLUSTERIP/** directory. Note: On Red Hat Enterprise 6, only root can write to files in the **/proc/net/ipt_CLUSTERIP/** directory by default. This update corrects this issue as a preventative measure in case an administrator has changed the permissions on these files. Red Hat would like to thank Vasiliy Kulikov for reporting this issue.

BZ#684275

Using the **pam_tty_audit.so** module (which enables or disables TTY auditing for specified users) in the **/etc/pam.d/sudo** file and in the **/etc/pam.d/system-auth** file when the audit package is not installed resulted in soft lock-ups on CPUs. As a result, the kernel became unresponsive. This was due to the kernel exiting immediately after TTY auditing was disabled, without emptying the buffer, which caused the kernel to spin in a loop, copying 0 bytes at each iteration and attempting to push each time without any effect. With this update, a locking mechanism is introduced to prevent the aforementioned behavior.

BZ#679306

Prior to this update, a collection of world-writable **sysfs** and **procfs** files allowed an unprivileged user to change various settings, change device hardware registers, and load certain firmware. With this update, permissions for these files have been changed.

BZ#694186

A previously introduced patch could cause **kswapd** (the kernel's memory reclaim daemon) to enter an infinite loop, consuming 100% of the CPU it is running on. This happened because **kswapd** incorrectly stayed awake for an unreclaimable zone. This update addresses this issue, and **kswapd** no longer consumes 100% of the CPU it is running on.

BZ#695322

If an error occurred during an I/O operation, the **SCSI** driver reset the **megaraid_sas** controller to restore it to normal state. However, on Red Hat Enterprise Linux 6, the waiting time to allow a full reset completion for the **megaraid_sas** controller was too short. The driver incorrectly recognized the controller as stalled, and, as a result, the system stalled as well. With this update, more time is given to the controller to properly restart, thus, the controller operates as expected after being reset.

Enhancement

BZ#683810

This update provides VLAN null tagging support (**VLAN ID 0** can be used in tags).

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. The system must be rebooted for this update to take effect.

B.38.7. RHBA-2012:0540 – kernel bug fix update

Updated kernel packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6 Extended Update Support.

[Updated 12 June 2012] This advisory has been updated with the correct description for bug 811297. The packages included in this revised update have not been changed in any way from the packages included in the original advisory.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Bug Fix

BZ#811297

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.

Enhancement

BZ#806904

The Intelligent Platform Management Interface (IPMI) specification requires a minimum communication timeout of five seconds. Previously, the kernel incorrectly used a timeout of 1 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.

All users of kernel are advised to upgrade to these updated packages, which fix this bug and add this enhancement. The system must be rebooted for this update to take effect.

B.38.8. RHBA-2012:0362 – 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.

Bug Fixes

BZ#771868

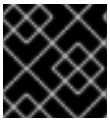
A bug in the splice code caused the file position on the write side of the sendfile() system call to be incorrectly set to the read-side file position. This could result in data being written to an incorrect offset of the destination file descriptor. With this update, sendfile() has been modified to correctly use the current file position for the write-side file descriptor. Note that the bug did not occur in the following sendfile() scenarios: when both read and write file positions were identical and when the file position was not important (for example if the write side was a socket).

BZ#786028

Previously, the sendfile(2) function was reimplemented to use splice infrastructure, but the function still checked for the f_op.sendpage() method call instead of the f_op.splice_write() method call. Because splice infrastructure was used for the sendfile(2) function, the check for sendpage infrastructure always failed. This problem has been fixed by removing the deprecated check and using f_op.sendpage() instead.

All users of kernel are advised to upgrade to these updated packages, which fix these bugs. Note that the system must be rebooted for this update to take effect.

B.38.9. RHSA-2011:0883 – Important: kernel security and bug fix update



IMPORTANT

This update has already been released as the security errata RHSA-2011:0883

Updated kernel packages that fix multiple security issues and three bugs are now available for Red Hat Enterprise Linux 6.0 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 after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update includes backported fixes for security issues. These issues, except for CVE-2011-1182, only affected users of Red Hat Enterprise Linux 6.0 Extended Update Support as they have already been addressed for users of Red Hat Enterprise Linux 6 in the 6.1 update, RHSA-2011:0542.

Security fixes

* Buffer overflow flaws were found in the Linux kernel's Management Module Support for Message Passing Technology (MPT) based controllers. A local, unprivileged user could use these flaws to cause a denial of service, an information leak, or escalate their privileges. (CVE-2011-1494, CVE-2011-1495, Important)

* A flaw was found in the Linux kernel's networking subsystem. If the number of packets received exceeded the receiver's buffer limit, they were queued in a backlog, consuming memory, instead of being discarded. A remote attacker could abuse this flaw to cause a denial of service (out-of-memory condition). (CVE-2010-4251, CVE-2010-4805, Moderate)

* A flaw was found in the Linux kernel's Transparent Huge Pages (THP) implementation. A local, unprivileged user could abuse this flaw to allow the user stack (when it is using huge pages) to grow and cause a denial of service. (CVE-2011-0999, Moderate)

* A flaw in the Linux kernel's Event Poll (epoll) implementation could allow a local, unprivileged user to cause a denial of service. (CVE-2011-1082, Moderate)

* An inconsistency was found in the interaction between the Linux kernel's method for allocating NFSv4 (Network File System version 4) ACL data and the method by which it was freed. This inconsistency led to a kernel panic which could be triggered by a local, unprivileged user with files owned by said user on an NFSv4 share. (CVE-2011-1090, Moderate)

* It was found that some structure padding and reserved fields in certain data structures in KVM (Kernel-based Virtual Machine) were not initialized properly before being copied to user-space. A privileged host user with access to **/dev/kvm** could use this flaw to leak kernel stack memory to user-space. (CVE-2010-3881, Low)

* A missing validation check was found in the Linux kernel's **mac_partition()** implementation, used for supporting file systems created on Mac OS operating systems. A local attacker could use this flaw to cause a denial of service by mounting a disk that contains specially-crafted partitions. (CVE-2011-1010, Low)

* A buffer overflow flaw in the DEC Alpha OSF partition implementation in the Linux kernel could allow a local attacker to cause an information leak by mounting a disk that contains specially-crafted partition tables. (CVE-2011-1163, Low)

* Missing validations of null-terminated string data structure elements in the **do_replace()**, **compat_do_replace()**, **do_ipt_get_ctl()**, **do_ip6t_get_ctl()**, and **do_arpt_get_ctl()** functions could allow a local user who has the **CAP_NET_ADMIN** capability to cause an information leak. (CVE-2011-1170, CVE-2011-1171, CVE-2011-1172, Low)

* A missing validation check was found in the Linux kernel's signals implementation. A local, unprivileged user could use this flaw to send signals via the **sigqueueinfo** system call, with the **si_code** set to ***SI_TKILL*** and with spoofed process and user IDs, to other processes. Note: This flaw does not allow existing permission checks to be bypassed; signals can only be sent if your privileges allow you to already do so. (CVE-2011-1182, Low)

Red Hat would like to thank Dan Rosenberg for reporting CVE-2011-1494 and CVE-2011-1495; Nelson Elhage for reporting CVE-2011-1082; Vasiliy Kulikov for reporting CVE-2010-3881, CVE-2011-1170, CVE-2011-1171, and CVE-2011-1172; Timo Warns for reporting CVE-2011-1010 and CVE-2011-1163; and Julien Tinnes of the Google Security Team for reporting CVE-2011-1182.

Bug fixes

BZ#590187

Previously, CPUs kept continuously locking up in the **inet_csk_bind_conflict()** function until the entire system became unreachable when all the CPUs were unresponsive due to a hash locking issue when using port redirection in the **__inet_inherit_port()** function. With this update, the underlying source code of the **__inet_inherit_port()** function has been modified to address this issue, and CPUs no longer lock up.

BZ#709380

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#706543

An **IDX ACTIVATE** timeout occurred during an online setting of an OSN device. This was because an incorrect function was provided on the **IDX ACTIVATE**. Because OSN devices use the same function level as OSD devices, this update adds OSN devices to the initialization function for the **func_level**; thus, resolving this issue.

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.

B.38.10. RHBA-2011:1495 – kernel bug fix update

Updated kernel packages that fix one bug 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 Fix

BZ#751081

When a host was in recovery mode and a SCSI scan operation was initiated, the scan operation failed and provided no error output. With this update, the underlying code has been modified, and the SCSI layer now waits for recovery of the host to complete scan operations for devices.

All users of kernel are advised to upgrade to these updated packages, which fix this bug. The system must be rebooted for this update to take effect.

B.38.11. RHBA-2011:1412 – kernel bug fix update

Updated kernel packages that fix one bug 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 Fix

BZ#695256

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.

All users of kernel are advised to upgrade to these updated packages, which fix this bug. The system must be rebooted for this update to take effect.

B.38.12. RHBA-2011:1283 – kernel bug fix update

Updated kernel packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Bug Fixes

BZ#731968

Prior to this update, a kernel panic could occur when the Intel 82599 Virtual Function driver was used from the guest. As a result, 10 gigabit Ethernet(10GbE) network interface cards (NICs) could not be used correctly. This update modifies the code so that 10GbE NICs can be used when they are operated from the guest.

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.

B.39. krb5

B.39.1. RHSA-2010:0863 – Important: 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 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.

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).

CVE-2010-1322

An uninitialized pointer use flaw was found in the way the MIT Kerberos KDC handled TGS (Ticket-granting Server) request messages. A remote, authenticated attacker could use this flaw to crash the KDC or, possibly, disclose KDC memory or execute arbitrary code with the privileges of the KDC (krb5kdc).

Red Hat would like to thank the MIT Kerberos Team for reporting this issue. Upstream acknowledges Mike Roszkowski as the original reporter.

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.

B.39.2. RHSA-2010:0925 – Important: krb5 security and bug fix update

Updated krb5 packages that fix multiple security issues and one bug 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.

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).

CVE-2010-1323, CVE-2010-1324, CVE-2010-4020

Multiple checksum validation flaws were discovered in the MIT Kerberos implementation. A remote attacker could use these flaws to tamper with certain Kerberos protocol packets and, possibly, bypass authentication or authorization mechanisms and escalate their privileges.

Red Hat would like to thank the MIT Kerberos Team for reporting these issues.

Bug Fix

BZ#644825

When attempting to perform PKINIT pre-authentication, if the client had more than one possible candidate certificate the client could fail to select the certificate and key to use. This usually occurred if certificate selection was configured to use the value of the keyUsage extension, or if any of the candidate certificates did not contain a subjectAltName extension. Consequently, the client attempted to perform pre-authentication using a different (usually password-based) mechanism.

All krb5 users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the krb5kdc daemon will be restarted automatically.

B.39.3. RHSA-2011:0200 – Important: krb5 security update

Updated krb5 packages that fix three 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.

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).

CVE-2011-0282

A NULL pointer dereference flaw was found in the way the MIT Kerberos KDC processed principal names that were not null terminated, when the KDC was configured to use an LDAP back end. A remote attacker could use this flaw to crash the KDC via a specially-crafted request.

CVE-2011-0281

A denial of service flaw was found in the way the MIT Kerberos KDC processed certain principal names when the KDC was configured to use an LDAP back end. A remote attacker could use this flaw to cause the KDC to hang via a specially-crafted request.

CVE-2010-4022

A denial of service flaw was found in the way the MIT Kerberos V5 slave KDC update server (kpropd) processed certain update requests for KDC database propagation. A remote attacker could use this flaw to terminate the kpropd daemon via a specially-crafted update request.

Red Hat would like to thank the MIT Kerberos Team for reporting the CVE-2011-0282 and CVE-2011-0281 issues. Upstream acknowledges Kevin Longfellow of Oracle Corporation as the original reporter of the CVE-2011-0281 issue.

All krb5 users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the krb5kdc daemon will be restarted automatically.

B.39.4. RHSA-2011:0356 – Important: 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 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.

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). The Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) capability provides support for using public-key authentication with Kerberos.

CVE-2011-0284

A double-free flaw was found in the way the MIT Kerberos KDC handled initial authentication requests (AS-REQ), when the KDC was configured to provide the PKINIT capability. A remote attacker could use this flaw to cause the KDC daemon to abort by using a specially-crafted AS-REQ request.

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.

B.39.5. RHSA-2011:0447 – 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).

CVE-2011-0285

An invalid free flaw was found in the password-changing capability of the MIT Kerberos administration daemon, kadmind. A remote, unauthenticated attacker could use this flaw to cause kadmind to abort via a specially-crafted request.

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the kadmind daemon will be restarted automatically.

B.40. libcap-ng

B.40.1. RHBA-2010:0906 – libcap-ng bug fix update

Updated libcap-ng packages that fix a bug are now available for Red Hat Enterprise Linux 6.

The libcap-ng library is designed to make programming with POSIX capabilities easier. It is shipped with utilities to analyze the POSIX capabilities of all running applications, as well as tools to set the file system-based capabilities.

Bug Fix

BZ#650131

Previously, when listing the file system based capabilities of a single file with the "filecap" utility, it would terminate with a segmentation fault. This error has been fixed, and "filecap" no longer crashes when attempting to list the capabilities of a single file.

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

B.41. libcgroup

B.41.1. RHSA-2011:0320 – Important: libcgroup security update

Updated libcgroup 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 libcgroup packages provide tools and libraries to control and monitor control groups.

CVE-2011-1006

A heap-based buffer overflow flaw was found in the way libcgroup converted a list of user-provided controllers for a particular task into an array of strings. A local attacker could use this flaw to escalate their privileges via a specially-crafted list of controllers.

CVE-2011-1022

It was discovered that libcgroup did not properly check the origin of Netlink messages. A local attacker could use this flaw to send crafted Netlink messages to the cgrulesengd daemon, causing it to put processes into one or more existing control groups, based on the attacker's choosing, possibly allowing the particular tasks to run with more resources (memory, CPU, etc.) than originally intended.

Red Hat would like to thank Nelson Elhage for reporting the CVE-2011-1006 issue.

All libcgroup users should upgrade to these updated packages, which contain backported patches to correct these issues.

B.42. libnl

B.42.1. RHBA-2011:0325 – libnl bug fix update

Updated libnl packages that fix a bug are now available for Red Hat Enterprise Linux 6.

The libnl package contains a convenience library to simplify using the Linux kernel netlink sockets interface for network manipulation.

Bug Fix

BZ#676327

Some nl_send_auto_complete() callers did not free the allocated message when errors were reported, resulting in libnl leaking memory. A problem in its own right, these small leaks also made it more work to detect memory leaks in other processes. With this update, allocated messages are freed correctly when nl_send_auto_complete() is called, and libnl no longer leaks memory in this circumstance.

All libnl users should upgrade to these updated packages, which fix this bug.

B.43. libtiff

B.43.1. RHSA-2011:0318 – Important: libtiff security update

Updated libtiff 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 libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

CVE-2011-0192

A heap-based buffer overflow flaw was found in the way libtiff processed certain TIFF Internet Fax image files, compressed with the CCITT Group 4 compression algorithm. An attacker could use this flaw to create a specially-crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code.

Red Hat would like to thank Apple Product Security for reporting this issue.

All libtiff users should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running applications linked against libtiff must be restarted for this update to take effect.

B.43.2. RHSA-2011:0392 – Important: libtiff security and bug fix update

Updated libtiff packages that fix one security issue and one bug 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 libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

CVE-2011-1167

A heap-based buffer overflow flaw was found in the way libtiff processed certain TIFF files encoded with a 4-bit run-length encoding scheme from ThunderScan. An attacker could use this flaw to create a specially-crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code.

Bug Fix

BZ#688825

The RHSA-2011:0318 libtiff update introduced a regression that prevented certain TIFF Internet Fax image files, compressed with the CCITT Group 4 compression algorithm, from being read.

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.

B.43.3. RHSA-2011:0452 – Important: libtiff security update

Updated libtiff 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.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

CVE-2009-5022

A heap-based buffer overflow flaw was found in the way libtiff processed certain TIFF image files that were compressed with the JPEG compression algorithm. An attacker could use this flaw 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 this issue. All running applications linked against libtiff must be restarted for this update to take effect.

B.44. libuser

B.44.1. RHSA-2011:0170 – Moderate: libuser security update

Updated libuser 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 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 libuser library implements a standardized interface for manipulating and administering user and group accounts. Sample applications that are modeled after applications from the shadow password suite (shadow-utils) are included in these packages.

CVE-2011-0002

It was discovered that libuser did not set the password entry correctly when creating LDAP (Lightweight Directory Access Protocol) users. If an administrator did not assign a password to an LDAP based user account, either at account creation with luseradd, or with lpasswd after account creation, an attacker could use this flaw to log into that account with a default password string that should have been rejected.

NOTE

Note that LDAP administrators that have used libuser tools to add users should check existing user accounts for plain text passwords, and reset them as necessary.

Users of libuser should upgrade to these updated packages, which contain a backported patch to correct this issue.

B.45. libvirt

B.45.1. RHSA-2011:0391 – Important: libvirt security update

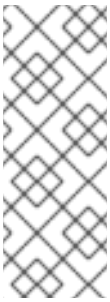
Updated libvirt packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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.

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 remotely managing virtualized systems.

CVE-2011-1146

It was found that several libvirt API calls did not honor the read-only permission for connections. A local attacker able to establish a read-only connection to libvirtd on a server could use this flaw to execute commands that should be restricted to read-write connections, possibly leading to a denial of service or privilege escalation.



NOTE

Previously, using rpmbuild without the '--define "rhel 5"' option to build the libvirt source RPM on Red Hat Enterprise Linux 5 failed with a "Failed build dependencies" error for the device-mapper-devel package, as this -devel sub-package is not available on Red Hat Enterprise Linux 5. With this update, the -devel sub-package is no longer checked by default as a dependency when building on Red Hat Enterprise Linux 5, allowing the libvirt source RPM to build as expected.

All libvirt users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, libvirtd must be restarted ("service libvirtd restart") for this update to take effect.

B.45.2. RHSA-2011:0479 – Moderate: libvirt security and bug fix update

Updated libvirt 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 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 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 remotely managing virtualized systems.

CVE-2011-1486

A flaw was found in the way libvirtd handled error reporting for concurrent connections. A remote attacker able to establish read-only connections to libvirtd on a server could use this flaw to crash libvirtd.

Bug Fix

BZ#668692

Previously, running qemu under a different UID prevented it from accessing files with mode 0660 permissions that were owned by a different user, but by a group that qemu was a member of.

All libvirt users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, libvirtd must be restarted ("service libvirtd restart") for this update to take effect.

B.45.3. RHBA-2011:0446 – libvirt bug fix update

Updated libvirt packages that fix multiple 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 remotely managing virtualized systems.

Bug Fixes

BZ#656355

When a root-squashing export of a domain was owned by a group to which the qemu user belonged, but was not owned by the qemu user, libvirt could not create a file to save the domain's state. This was because the save operation was invoked by the user who did not have the needed group permissions. With this update, libvirt first acquires all the needed group permissions and only then attempts to perform the aforementioned save operation.

BZ#656972

Members of the qemu group did not have read/write permissions for the "[localstatedir]/[cache/lib]/libvirt/qemu/" directory in which XML files which define sockets are placed. Permissions are now updated to allow the qemu group read/write permissions.

BZ#658141

A race condition where an application could query block information on a virtual guest that had just been migrated away could occur when migrating a guest. As a result, the libvirt service crashed. The libvirt application now verifies that a guest exists before attempting to start any monitoring operations.

BZ#658143

Live migration of a guest could take an exceptionally long time to converge to the switchover point if the guest was very busy. By allowing to increase the downtime setting of a guest, migration is more likely to complete. However, libvirt was sending an incorrectly formatted request to increase the downtime setting of a guest. With this update, libvirt correctly sends the downtime setting request.

BZ#658144

The "addrToString" methods did not work properly with UNIX domain sockets which did not have a normal "host:port" address. As a result SASL (Simple Authentication and Security Layer) could not be used over UNIX domain sockets. With this update, the "addrToString" methods are fixed and SASL is no longer restricted to TCP connections.

BZ#662042

Prior to this update, libvirt was not able to recognize whether a domain crashed or was properly shut down. With this update, a SHUTDOWN event sent by qemu is recognized by libvirt when a domain is properly shut down. If the SHUTDOWN event is not received, the domain is declared to have crashed.

BZ#662043

A deadlock occurred in the libvirt service when running concurrent bidirectional migration because certain calls did not release their local driver lock before issuing an RPC (Remote Procedure Call) call on a remote libvirt daemon. A deadlock no longer occurs between two communicating libvirt daemons.

BZ#662045

A specification file bug caused permissions on the /var/lib/libvirt directory to change when upgrading a system. With this update, correct permissions are assigned to the aforementioned directory.

BZ#662046

An off-by-one error in a clock variable caused a virtual guest to show incorrect date and time information. This update addresses this error. Date and time information is now correctly displayed.

BZ#668694

The %post script (part of the libvirt-client package) started the libvirt-guests service even when the service was explicitly turned off. With this update, the libvirt-guests service is no longer started when explicitly turned off.

BZ#672549

Starting and shutting down a domain led to a memory leak due to the memory buffer not being freed properly. With this update, starting and shutting down a domain no longer leads to a memory leak.

BZ#672554

Starting and shutting down a domain led to a memory leak due to the use of a thread-unfriendly "matchpathcon" (which gets the default security context for the specified path) SELinux API. With this update, libvirt uses improved SELinux APIs and a memory leak no longer occurs.

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

B.46. libvpx

B.46.1. RHSA-2010:0999 – Moderate: libvpx security update

Updated libvpx 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 libvpx packages provide the VP8 SDK, which allows the encoding and decoding of the VP8 video codec, commonly used with the WebM multimedia container file format.

CVE-2010-4203

An integer overflow flaw, leading to arbitrary memory writes, was found in libvpx. An attacker could create a specially-crafted video encoded using the VP8 codec that, when played by a victim with an application using libvpx (such as Totem), would cause the application to crash or, potentially, execute arbitrary code.

All users of libvpx are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, all applications using libvpx must be restarted for the changes to take effect.

B.47. lldpad

B.47.1. RHBA-2010:0857 – lldpad bug fix update

An updated lldpad package that fixes dcbx negotiation issues is now available for Red Hat Enterprise Linux 6.

The lldpad package adds Link Layer Discovery Protocol (LLDP) support for all ports.

Bug Fix

BZ#639414

Previously, lldpad failed to initiate a dcbx negotiation when a "link down" netlink event message was dropped or lost. As a result, a boot failure occurred and the system got suspended. With this update, lldpad dcbx negotiation works as expected.

All lldpad users are advised to upgrade to this updated package, which resolves this issue.

B.48. logrotate

B.48.1. RHSA-2011:0407 – Moderate: logrotate security update

An updated logrotate 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The logrotate utility simplifies the administration of multiple log files, allowing the automatic rotation, compression, removal, and mailing of log files.

CVE-2011-1154

A shell command injection flaw was found in the way logrotate handled the shred directive. A specially-crafted log file could cause logrotate to execute arbitrary commands with the privileges of the user running logrotate (root, by default). Note: The shred directive is not enabled by default.

CVE-2011-1098

A race condition flaw was found in the way logrotate applied permissions when creating new log files. In some specific configurations, a local attacker could use this flaw to open new log files before logrotate applies the final permissions, possibly leading to the disclosure of sensitive information.

CVE-2011-1155

An input sanitization flaw was found in logrotate. A log file with a specially-crafted file name could cause logrotate to abort when attempting to process that file a subsequent time.

All logrotate users should upgrade to this updated package, which contains backported patches to resolve these issues.

B.49. logwatch

B.49.1. RHSA-2011:0324 — Important: logwatch security update

An updated logwatch package that fixes one security issue is 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.

Logwatch is a customizable log analysis system. Logwatch parses through your system's logs for a given period of time and creates a report analyzing areas that you specify, in as much detail as you require.

CVE-2011-1018

A flaw was found in the way Logwatch processed log files. If an attacker were able to create a log file with a malicious file name, it could result in arbitrary code execution with the privileges of the root user when that log file is analyzed by Logwatch.

Users of logwatch should upgrade to this updated package, which contains a backported patch to resolve this issue.

B.50. luci

B.50.1. RHBA-2011:0906 — luci bug fix update

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

The luci package provides a web-based high-availability cluster configuration application.

Bug Fix

BZ#681764

When configuring a cluster, the graphical user interface of the luci application allows users to

configure fence agents. Previously, this interface did not include the fence_brocade agent in the list of available options. Since the RHBA-2011:0363 bug fix update re-included fence_brocade in the fence-agents package that is distributed with Red Hat Enterprise Linux 6, this update re-adds this agent (the "Brocade Fabric Switch" option) to the list of fence agents that are available for configuration.

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

B.50.2. RHBA-2010:0851 – luci bug fix update

An updated luci package that fix a bug are now available for Red Hat Enterprise Linux 6.

The luci package contains a web-based high availability cluster configuration application.

Bug Fix

BZ#642140

Previously, Luci did not allow users to configure unfencing. Due to this, SAN fencing agents and fence_scsi could not be unfenced on system boot. This update adds a default option for the SAN fence configuration pages that enable the unfencing functionality.

All luci users are advised to upgrade to this updated package, which fix this bug.

B.51. lvm2

B.51.1. RHEA-2010:0994 – lvm2 enhancement update

Updated lvm2 packages that add various enhancements are now available for Red Hat Enterprise Linux 6.

The lvm2 packages contain support for Logical Volume Management (LVM).

Enhancements

BZ#661741

Previously, the maximum length of a tag was limited to 128 characters. However, in certain cases, this may have been too restrictive. To remove this restriction, the lvm2 packages have been updated to support tags that are up to 1024 characters long.

BZ#661742

Due to technical limitations, a valid tag can consist of a limited range of characters only. With this update, the list of allowed characters has been extended, and tags can newly contain "/", "=", "!", ":", "#", and "&".

Users are advised to upgrade to these updated lvm2 packages, which add these enhancements.

B.51.2. RHBA-2010:0951 – lvm2 bug fix update and enhancement

Updated lvm2 packages that fix several bugs and add an enhancement are now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

Bug Fixes

BZ#651007

Merging of a snapshot volume caused I/O errors to be issued during a reboot. After the reboot the snapshot volume (snapshot of an LV where the root file system resides) was still present and it appeared as if the merge operation was still in progress. With this update, the errors no longer occur and the snapshot merge completes cleanly.

BZ#652185

The optimizer for the regex filter defined in the LVM2 configuration (the 'devices/filter' setting) did not work correctly when using the 'or' operator. This resulted in improper filtering of devices. With this update, the application of the regex filter works as expected.

BZ#652186

Previously, the 'vgchange' command did not allow the '--addtag' and '--deltag' arguments to be used simultaneously. With this update, this restriction is removed.

BZ#652638

Prior to this update, the 'fsadm' script issued an error message about not being able to resize the just unmounted file system because it required the 'force' option to be used. With this update, the 'force' option is not needed anymore and the script proceeds and successfully resizes the file system.

Enhancement

BZ#652662

This update adds support for using multiple "--addtag" and "--deltag" arguments within a single command.

Users are advised to upgrade to these updated lvm2 packages, which resolve these issues and add this enhancement.

B.51.3. RHBA-2010:0849 – lvm2 bug fix update

Updated lvm2 packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The lvm2 packages contain support for Logical Volume Management (LVM).

Bug Fixes

BZ#641461

This update avoids data corruption caused by a failure to detect that a filesystem being resized with 'fsadm' (or lvresize/lvreduce --resizefs) is mounted. The update also fixes various other problems in 'fsadm' including incorrect handling of user's break action, inconsistent processing of the '--dry-run' option, missing support for correctly passing the '--yes' option, and incorrect handling of the 'LVM_BINARY' environment variable.

BZ#641812

Under some circumstances, creating cluster mirrors with the '--nosync' option could cause I/O to become extremely slow. Note that this issue only effected I/O immediately after the creation of the mirror, and only when '--nosync' was used. With this update, I/O no longer runs slow in the aforementioned case.

BZ#641896

Previously, the limit for tags section in metadata was 4096 characters. When this limit was exceeded, the VG metadata were corrupted. With this update, the limitation has been removed and the limit is given by metadata size only.

BZ#648554

Previously, a limit for maximum output length in reporting functions (vgs, lvs) caused problems while using a large set of tags. With this update, the output lines in these reports are now limited by available memory only.

All users of lvm2 are advised to upgrade to these updated packages, which fix these bugs.

B.52. mailman

B.52.1. RHSA-2011:0308 – Moderate: mailman security update

An updated mailman 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mailman is a program used to help manage email discussion lists.

CVE-2011-0707

Multiple input sanitization flaws were found in the way Mailman displayed usernames of subscribed users on certain pages. If a user who is subscribed to a mailing list were able to trick a victim into visiting one of those pages, they could perform a cross-site scripting (XSS) attack against the victim.

CVE-2010-3089

Multiple input sanitization flaws were found in the way Mailman displayed mailing list information. A mailing list administrator could use this flaw to conduct a cross-site scripting (XSS) attack against victims viewing a list's "listinfo" page.

Red Hat would like to thank Mark Sapiro for reporting these issues.

Users of mailman should upgrade to this updated package, which contains backported patches to correct these issues.

B.53. mod_auth_mysql

B.53.1. RHSA-2010:1002 – Moderate: mod_auth_mysql security update

An updated mod_auth_mysql 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 mod_auth_mysql package includes an extension module for the Apache HTTP Server, which can be used to implement web user authentication against a MySQL database.

CVE-2008-2384

A flaw was found in the way mod_auth_mysql escaped certain multibyte-encoded strings. If mod_auth_mysql was configured to use a multibyte character set that allowed a backslash ("\") as part of the character encodings, a remote attacker could inject arbitrary SQL commands into a login request.

NOTE

Note that this flaw only affected non-default installations where AuthMySQLCharacterSet is configured to use one of the affected multibyte character sets. Installations that did not use the AuthMySQLCharacterSet configuration option were not vulnerable to this flaw.

All mod_auth_mysql users are advised to upgrade to this updated package, which contains a backported patch to correct this issue. After installing the updated package, the httpd daemon must be restarted for the update to take effect.

B.54. mysql

B.54.1. RHSA-2011:0164 – Moderate: mysql security update

Updated mysql 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 scores, 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.

CVE-2010-3840

The MySQL PolyFromWKB() function did not sanity check Well-Known Binary (WKB) data, which could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3839

A flaw in the way MySQL processed certain JOIN queries could allow a remote, authenticated attacker to cause excessive CPU use (up to 100%), if a stored procedure contained JOIN queries, and that procedure was executed twice in sequence.

CVE-2010-3838

A flaw in the way MySQL processed queries that provide a mixture of numeric and longblob data types to the LEAST or GREATEST function, could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3837

A flaw in the way MySQL processed PREPARE statements containing both GROUP_CONCAT and the WITH ROLLUP modifier could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3836

MySQL did not properly pre-evaluate LIKE arguments in view prepare mode, possibly allowing a remote, authenticated attacker to crash mysqld.

CVE-2010-3835

A flaw in the way MySQL processed statements that assign a value to a user-defined variable and that also contain a logical value evaluation could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3833

A flaw in the way MySQL evaluated the arguments of extreme-value functions, such as LEAST and GREATEST, could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3683

A flaw in the way MySQL handled LOAD DATA INFILE requests allowed MySQL to send OK packets even when there were errors.

CVE-2010-3682

A flaw in the way MySQL processed EXPLAIN statements for some complex SELECT queries could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3681

A flaw in the way MySQL processed certain alternating READ requests provided by HANDLER statements could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3680

A flaw in the way MySQL processed CREATE TEMPORARY TABLE statements that define NULL columns when using the InnoDB storage engine, could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3679

A flaw in the way MySQL processed certain values provided to the BINLOG statement caused MySQL to read unassigned memory. A remote, authenticated attacker could possibly use this flaw to crash mysqld.

CVE-2010-3678

A flaw in the way MySQL processed SQL queries containing IN or CASE statements, when a NULL argument was provided as one of the arguments to the query, could allow a remote, authenticated attacker to crash mysqld.

CVE-2010-3677

A flaw in the way MySQL processed JOIN queries that attempt to retrieve data from a unique SET column could allow a remote, authenticated attacker to crash mysqld.

NOTE

Note that CVE-2010-3840, CVE-2010-3838, CVE-2010-3837, CVE-2010-3835, CVE-2010-3833, CVE-2010-3682, CVE-2010-3681, CVE-2010-3680, CVE-2010-3678, and CVE-2010-3677 only cause a temporary denial of service, as mysqld was automatically restarted after each crash.

These updated packages upgrade MySQL to version 5.1.52. Refer to the MySQL release notes for a full list of changes:

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-52.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.

B.55. net-snmp

B.55.1. RHBA-2010:0901 – net-snmp bug fix update

Updated net-snmp packages that resolve several issues 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 MIB browser.

Bug Fixes

BZ#652223

The SNMP daemon, snmpd, returned the incorrect value of either "0.1" or 1.3" for sysObjectID. This update fixes the value of this OID so that the correct value, which is "1.3.6.1.4.1.8072.3.2.10", is now returned.

BZ#652551

Under certain conditions, and especially on networks with high traffic, snmpd wrote a lot of "c64 32 bit check failed" and "netsnmp_assert 1 == new_val->high failed" messages to the system log. Although these messages are harmless and not indicative of a serious error, they could potentially fill the system log quickly. This update suppresses these spurious messages in favor of more meaningful and specific error messages, which are written to the system log only once.

All users of net-snmp are advised to upgrade to these updated packages, which resolve these issues.

B.56. NetworkManager

B.56.1. RHBA-2010:0836 – NetworkManager bug fix and enhancement update

Updated NetworkManager packages that fix a bug 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 Fix

BZ#638598

Under certain circumstances, the "Enable Networking" and "Enable Wireless" menu items in the panel applet may have been insensitive. This error no longer occurs, and both options are now available as expected.

Enhancements

BZ#

In enterprise wireless networks, the proactive key caching can now be used along with the PEAP-GTC authentication mechanism.

BZ#

Punjabi translation of the network applet has been updated.

Users are advised to upgrade to these updated packages, which fix this bug and add these enhancements.

B.57. nss

B.57.1. RHSA-2010:0862 – Low: nss security update

Updated nss 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 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.

Network Security Services (NSS) is a set of libraries designed to support the development of security-enabled client and server applications.

CVE-2010-3170

A flaw was found in the way NSS matched SSL certificates when the certificates had a Common Name containing a wildcard and a partial IP address. NSS incorrectly accepted connections to IP addresses that fell within the SSL certificate's wildcard range as valid SSL connections, possibly allowing an attacker to conduct a man-in-the-middle attack.

All NSS users should upgrade to these updated packages, which provide NSS version 3.12.8 to resolve this issue. After installing the update, applications using NSS must be restarted for the changes to take effect.

B.57.2. RHSA-2011:0472 – Important: nss security update

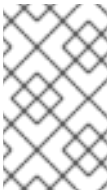
Updated nss packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact.

Network Security Services (NSS) is a set of libraries designed to support the development of security-enabled client and server applications.

BZ#689430

This erratum blacklists a small number of HTTPS certificates by adding them, flagged as untrusted, to the NSS Builtin Object Token (the libnssckbi.so library) certificate store.



NOTE

Note that this fix only applies to applications using the NSS Builtin Object Token. It does not blacklist the certificates for applications that use the NSS library, but do not use the NSS Builtin Object Token (such as curl).

All NSS users should upgrade to these updated packages, which correct this issue. After installing the update, applications using NSS must be restarted for the changes to take effect.

B.58. nss_db

B.58.1. RHBA-2011:0941 – nss_db bug fix update

An updated nss_db package that fixes a bug is now available for Red Hat Enterprise Linux 6 Extended Update Support.

The nss_db package contains a set of C library extensions 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 NIS (Network Information Service).

Bug Fix

BZ#718202

When a module does not provide its own method for retrieving a user's list of supplemental group memberships, the libc library's default method is used instead to get that information by examining all of the groups known to the module. Consequently, applications which attempted to retrieve the information from multiple threads simultaneously, interfered with each other and each received an incomplete result set. This update provides a module-specific method which prevents this interference in the nss_db module.

Users of nss_db are advised to upgrade to this updated package, which fixes this bug.

B.59. openldap

B.59.1. RHSA-2011:0347 – Moderate: openldap security update

Updated openldap packages that fix three 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools.

CVE-2011-1024

A flaw was found in the way OpenLDAP handled authentication failures being passed from an OpenLDAP slave to the master. If OpenLDAP was configured with a chain overlay and it forwarded authentication failures, OpenLDAP would bind to the directory as an anonymous user and return success, rather than return failure on the authenticated bind. This could allow a user on a system that uses LDAP for authentication to log into a directory-based account without knowing the password.

CVE-2011-1025

It was found that the OpenLDAP back-ndb back end allowed successful authentication to the root distinguished name (DN) when any string was provided as a password. A remote user could use this flaw to access an OpenLDAP directory if they knew the value of the root DN. Note: This issue only affected OpenLDAP installations using the NDB back-end, which is only available for Red Hat Enterprise Linux 6 via third-party software.

CVE-2011-1081

A flaw was found in the way OpenLDAP handled modify relative distinguished name (modrdn) requests. A remote, unauthenticated user could use this flaw to crash an OpenLDAP server via a modrdn request containing an empty old RDN value.

Users of OpenLDAP should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the OpenLDAP daemons will be restarted automatically.

B.60. openoffice.org

B.60.1. RHSA-2011:0183 – Important: openoffice.org security and bug fix update

Updated openoffice.org packages that fix multiple security issues and one bug 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.

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.

CVE-2010-3451, CVE-2010-3452

An array index error and an integer signedness error were found in the way OpenOffice.org parsed certain Rich Text Format (RTF) files. An attacker could use these flaws to create a specially-crafted RTF file that, when opened, would cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org.

CVE-2010-3453, CVE-2010-3454

A heap-based buffer overflow flaw and an array index error were found in the way OpenOffice.org parsed certain Microsoft Office Word documents. An attacker could use these flaws to create a specially-crafted Microsoft Office Word document that, when opened, would cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org.

CVE-2010-4253

A heap-based buffer overflow flaw was found in the way OpenOffice.org parsed certain Microsoft

Office PowerPoint files. An attacker could use this flaw to create a specially-crafted Microsoft Office PowerPoint file that, when opened, would cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org.

CVE-2010-4643

A heap-based buffer overflow flaw was found in the way OpenOffice.org parsed certain TARGA (Truevision TGA) files. An attacker could use this flaw to create a specially-crafted TARGA file. If a document containing this specially-crafted TARGA file was opened, or if a user tried to insert the file into an existing document, it would cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org.

CVE-2010-3450

A directory traversal flaw was found in the way OpenOffice.org handled the installation of XSLT filter descriptions packaged in Java Archive (JAR) files, as well as the installation of OpenOffice.org Extension (.oxt) files. An attacker could use these flaws to create a specially-crafted XSLT filter description or extension file that, when opened, would cause the OpenOffice.org Extension Manager to modify files accessible to the user installing the JAR or extension file.

CVE-2010-3689

A flaw was found in the script that launches OpenOffice.org. In some situations, a "." character could be included in the LD_LIBRARY_PATH variable, allowing a local attacker to execute arbitrary code with the privileges of the user running OpenOffice.org, if that user ran OpenOffice.org from within an attacker-controlled directory.

Red Hat would like to thank OpenOffice.org for reporting the CVE-2010-3451, CVE-2010-3452, CVE-2010-3453, CVE-2010-3454, and CVE-2010-4643 issues; and Dmitri Gribenko for reporting the CVE-2010-3689 issue. Upstream acknowledges Dan Rosenberg of Virtual Security Research as the original reporter of the CVE-2010-3451, CVE-2010-3452, CVE-2010-3453, and CVE-2010-3454 issues.

Bug Fix

BZ#671087

OpenOffice.org did not create a lock file when opening a file that was on a share mounted via SFTP. Additionally, if there was a lock file, it was ignored. This could result in data loss if a file in this situation was opened simultaneously by another user.

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.

B.61. openssh

B.61.1. RHBA-2010:0943 – openssh bug fix update

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

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

Bug Fixes

BZ#651820

When the ~/.bashrc startup file contained a command that produced an output to standard error (STDERR), the sftp utility was unable to log in to that account. This bug has been fixed, and the output to STDERR no longer prevents sftp from establishing the connection.

BZ#655043

Prior to this update, the authentication based on a GSS key exchange did not work, rendering users unable to authenticate using this method. With this update, the underlying source code has been modified to target this issue, and the GSSKEX-based authentication now works as expected.

All OpenSSH users are advised to upgrade to these updated packages, which resolve these issues.

B.62. openssl

B.62.1. RHSA-2010:0888 – Important: openssl security update

Updated openssl 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.

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.

CVE-2010-3864

A race condition flaw has been found in the OpenSSL TLS server extension parsing code, which could affect some multithreaded OpenSSL applications. Under certain specific conditions, it may be possible for a remote attacker to trigger this race condition and cause such an application to crash, or possibly execute arbitrary code with the permissions of the application.

NOTE

Note that this issue does not affect the Apache HTTP Server. Refer to Red Hat Bugzilla bug 649304 for more technical details on how to determine if your application is affected.

Red Hat would like to thank Rob Hulswit for reporting this issue.

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.

B.62.2. RHSA-2010:0979 – Moderate: openssl security update

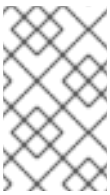
Updated openssl packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

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.

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.

CVE-2010-4180

A ciphersuite downgrade flaw was found in the OpenSSL SSL/TLS server code. A remote attacker could possibly use this flaw to change the ciphersuite associated with a cached session stored on the server, if the server enabled the SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG option, possibly forcing the client to use a weaker ciphersuite after resuming the session.



NOTE

Note that with this update, setting the SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG option has no effect and this bug workaround can no longer be enabled.

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.

B.63. openswan

B.63.1. RHSA-2010:0892 – Moderate: openswan security update

Updated openswan 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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.

CVE-2010-3302, CVE-2010-3308

Two buffer overflow flaws were found in the Openswan client-side XAUTH handling code used when connecting to certain Cisco gateways. A malicious or compromised VPN gateway could use these flaws to execute arbitrary code on the connecting Openswan client.

CVE-2010-3752, CVE-2010-3753

Two input sanitization flaws were found in the Openswan client-side handling of Cisco gateway banners. A malicious or compromised VPN gateway could use these flaws to execute arbitrary code on the connecting Openswan client.

Red Hat would like to thank the Openswan project for reporting these issues. Upstream acknowledges D. Hugh Redelmeier and Paul Wouters as the original reporters.

All users of openswan are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the ipsec service will be restarted automatically.

B.64. pam

B.64.1. RHSA-2010:0891 – Moderate: pam security update

Updated pam packages that fix three 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Pluggable Authentication Modules (PAM) provide a system whereby administrators can set up authentication policies without having to recompile programs that handle authentication.

CVE-2010-3853

It was discovered that the pam_namespace module executed the external script namespace.init with an unchanged environment inherited from an application calling PAM. In cases where such an environment was untrusted (for example, when pam_namespace was configured for setuid applications such as su or sudo), a local, unprivileged user could possibly use this flaw to escalate their privileges.

CVE-2010-3435

It was discovered that the pam_env and pam_mail modules used root privileges while accessing user's files. A local, unprivileged user could use this flaw to obtain information, from the lines that have the KEY=VALUE format expected by pam_env, from an arbitrary file. Also, in certain configurations, a local, unprivileged user using a service for which the pam_mail module was configured for, could use this flaw to obtain limited information about files or directories that they do not have access to.

CVE-2010-3316

Note: As part of the fix for CVE-2010-3435, this update changes the default value of pam_env's configuration option user_readenv to 0, causing the module to not read user's ~/.pam_environment configuration file by default, as reading it may introduce unexpected changes to the environment of the service using PAM, or PAM modules consulted after pam_env.

It was discovered that the pam_xauth module did not verify the return values of the setuid() and setgid() system calls. A local, unprivileged user could use this flaw to execute the xauth command with root privileges and make it read an arbitrary input file.

Red Hat would like to thank Sebastian Krahmer of the SuSE Security Team for reporting the CVE-2010-3435 issue.

All pam users should upgrade to these updated packages, which contain backported patches to correct these issues.

B.65. pango

B.65.1. RHSA-2011:0180 – Moderate: pango security update

Updated pango and evolution28-pango 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 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.

Pango is a library used for the layout and rendering of internationalized text.

CVE-2011-0020

An input sanitization flaw, leading to a heap-based buffer overflow, was found in the way Pango displayed font files when using the FreeType font engine back end. If a user loaded a malformed font file with an application that uses Pango, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of pango and evolution28-pango are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, you must restart your system or restart your X session for the update to take effect.

B.65.2. RHSA-2011:0309 — Critical: pango security update

Updated pango 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 for each vulnerability from the CVE link(s) associated with each description below.

Pango is a library used for the layout and rendering of internationalized text.

CVE-2011-0064

It was discovered that Pango did not check for memory reallocation failures in the hb_buffer_ensure() function. An attacker able to trigger a reallocation failure by passing sufficiently large input to an application using Pango could use this flaw to crash the application or, possibly, execute arbitrary code with the privileges of the user running the application.

Red Hat would like to thank the Mozilla Security Team for reporting this issue.

All pango users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, you must restart your system or restart the X server for the update to take effect.

B.66. php

B.66.1. RHSA-2011:0195 — Moderate: php security update

Updated php 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 scores, 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.

CVE-2010-4645

A flaw was found in the way PHP converted certain floating point values from string representation to a number. If a PHP script evaluated an attacker's input in a numeric context, the PHP interpreter could cause high CPU usage until the script execution time limit is reached. This issue only affected i386 systems.

CVE-2009-5016, CVE-2010-3870

A numeric truncation error and an input validation flaw were found in the way the PHP utf8_decode()

function decoded partial multi-byte sequences for some multi-byte encodings, sending them to output without them being escaped. An attacker could use these flaws to perform a cross-site scripting attack.

CVE-2010-3709

A NULL pointer dereference flaw was found in the PHP ZipArchive::getArchiveComment function. If a script used this function to inspect a specially-crafted ZIP archive file, it could cause the PHP interpreter to crash.

All 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.

B.67. pidgin

B.67.1. RHSA-2010:0890 — 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. 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.

Pidgin is an instant messaging program which can log in to multiple accounts on multiple instant messaging networks simultaneously.

CVE-2010-3711

Multiple NULL pointer dereference flaws were found in the way Pidgin handled Base64 decoding. A remote attacker could use these flaws to crash Pidgin if the target Pidgin user was using the Yahoo! Messenger Protocol, MSN, MySpace, or Extensible Messaging and Presence Protocol (XMPP) protocol plug-ins, or using the Microsoft NT LAN Manager (NTLM) protocol for authentication.

Red Hat would like to thank the Pidgin project for reporting these issues. Upstream acknowledges Daniel Atallah as the original reporter.

All Pidgin users should upgrade to these updated packages, which contain a backported patch to resolve these issues. Pidgin must be restarted for this update to take effect.

B.68. pixman

B.68.1. RHBA-2010:0905 — pixman bug fix update

An updated pixman package is now available for Red Hat Enterprise Linux 6.

Pixman is a pixel manipulation library for the X Window System and cairo.

Bug Fix

BZ#644818

The pixman package has been updated to version 0.18, which provides new functionality that is required by SPICE, a remote display protocol used in Red Hat Enterprise Linux for viewing virtualized guests.

All users requiring SPICE are advised to upgrade to this updated package, which resolves this issue.

B.69. policycoreutils

B.69.1. RHSA-2011:0414 – Important: policycoreutils security update

Updated policycoreutils 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.

The policycoreutils packages contain the core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system and its policies.

CVE-2011-1011

It was discovered that the seunshare utility did not enforce proper file permissions on the directory used as an alternate temporary directory mounted as /tmp/. A local user could use this flaw to overwrite files or, possibly, execute arbitrary code with the privileges of a setuid or setgid application that relies on proper /tmp/ permissions, by running that application via seunshare.

Red Hat would like to thank Tavis Ormandy for reporting this issue.

This update also introduces the following changes:

* The seunshare utility was moved from the main policycoreutils subpackage to the policycoreutils-sandbox subpackage. This utility is only required by the sandbox feature and does not need to be installed by default.

* Updated selinux-policy packages that add the SELinux policy changes required by the seunshare fixes.

All policycoreutils users should upgrade to these updated packages, which correct this issue.

B.70. polkit

B.70.1. RHSA-2011:0455 – Important: polkit security update

Updated polkit 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.

PolicyKit is a toolkit for defining and handling authorizations.

CVE-2011-1485

A race condition flaw was found in the PolicyKit pkexec utility and polkitd daemon. A local user could use this flaw to appear as a privileged user to pkexec, allowing them to execute arbitrary commands as root by running those commands with pkexec.

Red Hat would like to thank Neel Mehta of Google for reporting this issue.

All polkit users should upgrade to these updated packages, which contain backported patches to correct this issue. The system must be rebooted for this update to take effect.

B.71. poppler

B.71.1. RHSA-2010:0859 – Important: poppler security update

Updated poppler packages that fix three 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.

Poppler is a Portable Document Format (PDF) rendering library, used by applications such as Evince.

CVE-2010-3702, CVE-2010-3703

Two uninitialized pointer use flaws were discovered in poppler. An attacker could create a malicious PDF file that, when opened, would cause applications that use poppler (such as Evince) to crash or, potentially, execute arbitrary code.

CVE-2010-3704

An array index error was found in the way poppler parsed PostScript Type 1 fonts embedded in PDF documents. An attacker could create a malicious PDF file that, when opened, would cause applications that use poppler (such as Evince) to crash or, potentially, execute arbitrary code.

Users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

B.72. postfix

B.72.1. RHSA-2011:0423 – Moderate: postfix security update

Updated postfix 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.

Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), and TLS.

CVE-2011-0411

It was discovered that Postfix did not flush the received SMTP commands buffer after switching to TLS encryption for an SMTP session. A man-in-the-middle attacker could use this flaw to inject SMTP commands into a victim's session during the plain text phase. This would lead to those

commands being processed by Postfix after TLS encryption is enabled, possibly allowing the attacker to steal the victim's mail or authentication credentials.

Red Hat would like to thank the CERT/CC for reporting CVE-2011-0411. The CERT/CC acknowledges Wietse Venema as the original reporter.

Users of Postfix are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the postfix service will be restarted automatically.

B.73. postgresql

B.73.1. RHSA-2010:0908 – Moderate: postgresql security update

Updated postgresql 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.

PostgreSQL is an advanced object-relational database management system (DBMS). PL/Perl and PL/Tcl allow users to write PostgreSQL functions in the Perl and Tcl languages. The PostgreSQL SECURITY DEFINER parameter, which can be used when creating a new PostgreSQL function, specifies that the function will be executed with the privileges of the user that created it.

CVE-2010-3433

It was discovered that a user could utilize the features of the PL/Perl and PL/Tcl languages to modify the behavior of a SECURITY DEFINER function created by a different user. If the PL/Perl or PL/Tcl language was used to implement a SECURITY DEFINER function, an authenticated database user could use a PL/Perl or PL/Tcl script to modify the behavior of that function during subsequent calls in the same session. This would result in the modified or injected code also being executed with the privileges of the user who created the SECURITY DEFINER function, possibly leading to privilege escalation.

These updated postgresql packages upgrade PostgreSQL to version 8.4.5. Refer to the PostgreSQL Release Notes for a 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 this issue. If the postgresql service is running, it will be automatically restarted after installing this update.

B.73.2. RHSA-2011:0197 – Moderate: postgresql security update

Updated postgresql 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 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.

PostgreSQL is an advanced object-relational database management system (DBMS).

CVE-2010-4015

A stack-based buffer overflow flaw was found in the way PostgreSQL processed certain tokens from an SQL query when the intarray module was enabled on a particular database. An authenticated database user running a specially-crafted SQL query could use this flaw to cause a temporary denial of service (postgres daemon crash) or, potentially, execute arbitrary code with the privileges of the database server.

Red Hat would like to thank Geoff Keating of the Apple Product Security team for reporting this issue.

For Red Hat Enterprise Linux 4, the updated postgresql packages contain a backported patch for this issue; there are no other changes.

For Red Hat Enterprise Linux 5, the updated postgresql packages upgrade PostgreSQL to version 8.1.23, and contain a backported patch for this issue. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.1/static/release.html

For Red Hat Enterprise Linux 6, the updated postgresql packages upgrade PostgreSQL to version 8.4.7, which includes a fix for this issue. 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 this issue. If the postgresql service is running, it will be automatically restarted after installing this update.

B.74. psmisc

B.74.1. RHBA-2011:0171 – psmisc bug fix update

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

The psmisc package contains utilities for managing processes on your system: pstree, killall, fuser and peekfd. The pstree command displays a tree structure of all of the running processes on your system. The killall command sends a specified signal (SIGTERM if nothing is specified) to processes identified by name. The fuser command identifies the PIDs of processes that are using specified files or file systems. The peekfd command attaches to a running process and intercepts all reads and writes to file descriptors.

Bug Fixes

BZ#668989

Due to an error in memory allocation, an attempt to kill a process group by using the "killall -g" command could fail. With this update, the memory allocation has been corrected, and the killall utility now works as expected.

BZ#668992

When parsing a list of command line arguments, the peekfd utility incorrectly used a wrong index. As a result, running the peekfd command with a file descriptor specified caused the utility to terminate unexpectedly with a segmentation fault. This update corrects this error, and the peekfd utility no longer fails to run.

All users of psmisc are advised to upgrade to this updated package, which resolves these issues.

B.75. python

B.75.1. RHBA-2011:0284 – python bug fix update

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

Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme, or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems such as X11, Motif, Tk, Mac, and MFC.

Bug Fixes

BZ#668975

Prior to this update, Python programs that used "ulimit -n" to enable communication with large numbers of subprocesses could still monitor only 1024 file descriptors at a time, which caused an exception:

ValueError: filedescriptor out of range in select()

This was due to the subprocess module using the "select" system call. The module now uses the "poll" system call, removing this limitation.

BZ#671343

Due to the urllib2 module ignoring the "no_proxy" environment variable for the FTP scheme, programs such as Yum could erroneously access a proxy server for ftp:// URLs covered by a "no_proxy" exclusion. With this update, a patch has been applied to address this issue, and "no_proxy" is no longer ignored.

All users of python are advised to upgrade to these updated packages, which resolve these issues.

B.76. python-dmidecode

B.76.1. RHBA-2011:1157 – python-dmidecode bug fix update

An updated python-dmidecode package that fixes a bug is now available for Red Hat Enterprise Linux 6 Extended Update Support.

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.

Bug Fix

BZ#726613

Previously, certain DMI (Direct Media Interface) tables did not report CPU information as a string and returned the NULL value instead. Consequently, Python terminated unexpectedly with a segmentation fault when trying to identify the CPU type by performing a string comparison. With this update, additional checks for NULL values, performed prior the string comparison, have been added to the code, thus fixing this bug.

All users of python-dmidecode are advised to upgrade to this updated package, which fixes this bug.

B.77. python-gudev

B.77.1. RHBA-2010:0850 – python-gudev bug fix update

An updated python-gudev package that fixes a bug is now available for Red Hat Enterprise Linux 6.

Python-gudev is one of the core components for Red Hat Network (RHN) registration process.

Bug Fix

BZ#637084

Under some circumstances, using the 'rhn_register' command to register a system with the Red Hat Network (RHN) might fail. When this issue is encountered, the 'rhn_register' command will return an error similar to:

```
# rhn_register
Segmentation fault (core dumped)
```

or

```
# rhn_register
***MEMORY-ERROR***: rhn_register[11525]: GSlice: assertion failed:
sinfo->n_allocated > 0
Aborted (core dumped)
```

With this update, the aforementioned errors are no longer returned and using the 'rhn_register' command works as expected.

All users of python-gudev are advised to upgrade to this updated package, which resolves this issue.

B.78. qemu-kvm

B.78.1. RHSA-2011:0345 – Moderate: 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 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.

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. Virtual Network Computing (VNC) is a remote display system.

CVE-2011-0011

A flaw was found in the way the VNC "password" option was handled. Clearing a password disabled VNC authentication, allowing a remote user able to connect to the virtual machines' VNC ports to open a VNC session without authentication.

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.

B.78.2. RHBA-2011:0012 – qemu-kvm bug fix update

Updated qemu-kvm packages that fix various 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. qemu-kvm is the user-space component for running virtual machines using KVM.

Bug Fixes

BZ#648821

When running a Windows Server 2008 virtual machine with a virtio network interface controller (NIC), unplugging the NIC could cause qemu-kvm to terminate unexpectedly with a segmentation fault. With this update, the underlying source code has been modified to address this issue, and unplugging such NIC while the virtual machine is active no longer causes qemu-kvm to crash.

BZ#653329

Previously, qemu-kvm did not allow a user to select a resolution higher than 1920x1080, which may have been rather limiting. This update increases the maximum supported resolution to 2560x1600.

BZ#653337

Due to an error in the Russian keyboard layout, pressing the "/" and "|" keys with the "ru" layout enabled produced wrong characters. With this update, the relevant lines in the ru.orig file have been corrected, and pressing these keys now produces the expected results.

BZ#653341

Under certain circumstances, QEMU could stop responding during the installation of an operating system in a virtual machine when the QXL display device was in use. This error no longer occurs, and kvm-qemu now works as expected.

BZ#653343

When running a virtual machine with 4 or more gigabytes of the virtual memory, an attempt to hot plug a network interface controller (NIC) failed with the following error message:

Device '[device_name]' could not be initialized

This update resolves this issue, and hot-plugging a NIC in a virtual machine with 4 or more gigabytes of the virtual memory no longer fails.

BZ#662058

Previously, the conversion of a disk image by using the "qemu-img convert" command may have been significantly slow. With this update, various patches have been applied to improve the performance of the above command.

All users of qemu-kvm are advised to upgrade to these updated packages, which resolve these issues.

B.78.3. RHBA-2010:0855 – qemu-kvm bug fix update

Updated qemu-kvm packages that fix various 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. qemu-kvm is the user-space component for running virtual machines using KVM.

Bug Fixes

BZ#633963

Prior to this update, virtio-net used a packet transmission algorithm that was using a timer to delay a transmission in an attempt to batch multiple packets together. However, this typically resulted in a higher latency. With this update, the default algorithm has been changed to use an asynchronous bottom half transmitter, improving the performance.

BZ#634249

Due to error in the committed_memory() function, the ksmtuned service was unable to determine the correct amount of memory used by qemu-kvm processes when no such process existed. This has been fixed, the relevant part of the source code has been corrected to return 0 when no qemu-kvm process is found, and ksmtuned now works as expected.

BZ#641835

Previously, attempting to commit a copy-on-write image to a raw backing disk image using the "quemu-img commit" command may have failed with the following error:

```
qemu-img: Error while committing image
```

With this update, this error no longer occurs, and such images can now be committed as expected.

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

B.79. quagga

B.79.1. RHSA-2010:0945 – Moderate: quagga security update

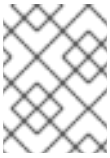
Updated quagga packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

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

Quagga is a TCP/IP based routing software suite. The Quagga bgpd daemon implements the BGP (Border Gateway Protocol) routing protocol.

CVE-2010-2948

A stack-based buffer overflow flaw was found in the way the Quagga bgpd daemon processed certain BGP Route Refresh (RR) messages. A configured BGP peer could send a specially-crafted BGP message, causing bgpd on a target system to crash or, possibly, execute arbitrary code with the privileges of the user running bgpd.



NOTE

Note that on Red Hat Enterprise Linux 6 it is not possible to exploit CVE-2010-2948 to run arbitrary code as the overflow is blocked by FORTIFY_SOURCE.

CVE-2010-2949

A NULL pointer dereference flaw was found in the way the Quagga bgpd daemon parsed the paths of autonomous systems (AS). A configured BGP peer could crash bgpd on a target system via a specially-crafted BGP message.

Users of quagga should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the bgpd daemon must be restarted for the update to take effect.

B.79.2. RHSA-2011:0406 – Moderate: quagga security update

Updated quagga 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Quagga is a TCP/IP based routing software suite. The Quagga bgpd daemon implements the BGP (Border Gateway Protocol) routing protocol.

CVE-2010-1675

A denial of service flaw was found in the way the Quagga bgpd daemon processed certain route metrics information. A BGP message with a specially-crafted path limit attribute would cause the bgpd daemon to reset its session with the peer through which this message was received.

CVE-2010-1674

A NULL pointer dereference flaw was found in the way the Quagga bgpd daemon processed malformed route extended communities attributes. A configured BGP peer could crash bgpd on a target system via a specially-crafted BGP message.

Users of quagga should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the bgpd daemon must be restarted for the update to take effect.

B.80. rdesktop

B.80.1. RHSA-2011:0506 – Moderate: rdesktop security update

An updated rdesktop package that fixes one security issue is 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.

rdesktop is a client for the Remote Desktop Server (previously, Terminal Server) in Microsoft Windows. It uses the Remote Desktop Protocol (RDP) to remotely present a user's desktop.

CVE-2011-1595

A directory traversal flaw was found in the way rdesktop shared a local path with a remote server. If a user connects to a malicious server with rdesktop, the server could use this flaw to cause rdesktop to read and write to arbitrary, local files accessible to the user running rdesktop.

Red Hat would like to thank Cendio AB for reporting this issue. Cendio AB acknowledges an anonymous contributor working with the SecuriTeam Secure Disclosure program as the original reporter.

Users of rdesktop should upgrade to this updated package, which contains a backported patch to resolve this issue.

B.81. resource-agents

B.81.1. RHBA-2010:0835 – resource-agents bug fix update

Updated resource-agents packages that provide a fix for a bug are now available for Red Hat Enterprise Linux 6.

The resource-agents packages contain the cluster resource agents for use by rgmanager and pacemaker. These agents allow users to build highly available services.

Bug Fix

BZ#640190

The config-utils library did not work correctly with certain references, causing problems with several agents.

All users of the resource-agents package are advised to upgrade to these updated packages, which address this issue and add this enhancement.

B.82. rsync

B.82.1. RHSA-2011:0390 – Moderate: rsync security update

An updated rsync 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.

rsync is a program for synchronizing files over a network.

CVE-2011-1097

A memory corruption flaw was found in the way the rsync client processed malformed file list data. If an rsync client used the "--recursive" and "--delete" options without the "--owner" option when connecting to a malicious rsync server, the malicious server could cause rsync on the client system to crash or, possibly, execute arbitrary code with the privileges of the user running rsync.

Red Hat would like to thank Wayne Davison and Matt McCutchen for reporting this issue.

Users of rsync should upgrade to this updated package, which contains a backported patch to resolve this issue.

B.83. ruby

B.83.1. RHBA-2011:0005 – ruby bug fix update

Updated ruby packages that fix a 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#653824

Under some circumstances on the PowerPC 64 architecture, Ruby did not save the context correctly before switching threads. Consequently, when a thread was restored, it had stale context whose use would result in a segmentation fault. This affected nearly any thread-using program on PowerPC 64. With this update, the underlying source code has been modified to address this issue, and the context is now saved correctly.

All PowerPC 64 ruby users are advised to upgrade to these updated packages, which resolve this issue.

B.84. samba

B.84.1. RHSA-2010:0860 – Critical: samba security update

Updated samba 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 for each vulnerability from the CVE link(s) associated with each description below.

Samba is a suite of programs used by machines to share files, printers, and other information.

CVE-2010-3069

A missing array boundary checking flaw was found in the way Samba parsed the binary representation of Windows security identifiers (SIDs). A malicious client could send a specially-crafted SMB request to the Samba server, resulting in arbitrary code execution with the privileges of the Samba server (smbd).

Users of Samba are advised to upgrade to these updated packages, which correct this issue. After installing this update, the smb service will be restarted automatically.

B.84.2. RHSA-2011:0305 – Important: samba security update

Updated samba 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.

Samba is a suite of programs used by machines to share files, printers, and other information.

CVE-2011-0719

A flaw was found in the way Samba handled file descriptors. If an attacker were able to open a large number of file descriptors on the Samba server, they could flip certain stack bits to "1" values, resulting in the Samba server (smbd) crashing.

Red Hat would like to thank the Samba team for reporting this issue.

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.

B.85. scsi-target-utils

B.85.1. RHSA-2011:0332 – Important: scsi-target-utils security update

An updated scsi-target-utils package that fixes one security issue is 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 scsi-target-utils package contains the daemon and tools to set up and monitor SCSI targets. Currently, iSCSI software and iSER targets are supported.

CVE-2011-0001

A double-free flaw was found in scsi-target-utils' tgtd daemon. A remote attacker could trigger this flaw by sending carefully-crafted network traffic, causing the tgtd daemon to crash.

Red Hat would like to thank Emmanuel Bouillon of NATO C3 Agency for reporting this issue.

All scsi-target-utils users should upgrade to this updated package, which contains a backported patch to correct this issue. All running scsi-target-utils services must be restarted for the update to take effect.

B.86. selinux-policy

B.86.1. RHBA-2010:0845 – selinux-policy bug fix update

Updated selinux-policy packages that fix various bugs are now available.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#637081

Due to incorrect SELinux policy, attempting to use the guest operating system customization in vCenter failed. With this update, the relevant policy code has been added, and SELinux no longer prevents users from customizing guest operating systems.

BZ#637082

When SELinux was enabled, suspending VMware virtual machines was either slowed down, or failed. With this update, the relevant policy has been corrected, and VMware virtual machines are now suspended as expected.

BZ#636489

When the cluster was configured to use fence_scsi, running the cman startup script or using the "fence_node -U <nodename>" command failed. These updated selinux-policy packages contain updated SELinux rules and add the security file context for the /var/lib/cluster directory, which

allows the cluster with fence_scsi enabled to work properly.

BZ#636488

Previously, the "allow_corosync_rw_tmpfs" boolean allowed third party applications to create, write and read generic tmpfs files. To prevent this, the boolean has been removed, and unless the unconfined policy is disabled, generic tmpfs files can now be managed using Corosync.

BZ#642607

Due to SELinux policies, certmonger was not permitted to search through directories that contain certificates. This error has been fixed, and selinux-policy packages now contain updated SELinux rules, which allow certmonger to access these directories.

BZ#642609

When SELinux was enabled, users were unable to mount GFS2 file systems listed in /etc/fstab. With this update, SELinux rules have been added to allow the mount process to communicate with gfs_controld, so that such file systems can now be mount as expected.

BZ#644807

Due to incorrect SELinux policy, smbcontrol, a utility that sends messages to the smbd, nmbd, or winbindd service, did not work properly. This error has been fixed, the relevant policy code has been added, and SELinux no longer prevents smbcontrol from working.

BZ#644808

With SELinux running in the enforcing mode, resuming the system from the Suspend mode failed, because the /etc/resolv.conf file did not have the correct security context. This was caused by NetworkManager, which was running under wrong SELinux domain, "devicekit_power_t". With this update, the proper SELinux domain transition from DeviceKit-power to NetworkManager has been added, and resuming from the Suspend mode now works as expected.

BZ#644820

Prior to this update, running the passwd command in the single user mode (that is, runlevel 1) failed when SELinux was enabled. To address this issue, the SELinux rules have been updated, so that passwd can now access the console, as well as all terminals (TTYs) and pseudo terminals (PTYs).

BZ#645658

Due to SELinux policy rules, certain iptables commands such as "iptables-save" or "iptables -L" were unable to write to files with output redirection. With this update, the SELinux domain transition from "unconfined_t" to the "iptables_t" domain has been removed, and such commands now work as expected.

All users of selinux-policy are advised to upgrade to these updated packages, which resolve these issues.

B.87. spice-client

B.87.1. RHEA-2010:0932 – spice-client enhancement update

An enhanced spice-client package is 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. SPICE users can view a virtualized desktop or server from the local system or any system with network access to the server. SPICE is available for a variety of machine architectures and operating systems. 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-client package provides the client side of the SPICE protocol.

Enhancement

BZ#644840

This update rebases spice-client to the 0.6.3 version. It is compatible with future spice protocol changes, it adds copy and paste support between guest and client (when used together with an updated agent), and supports fullscreen mode under window-managers other then the default Gnome window manager metacity (especially compiz and kde are now also supported).

All users requiring spice-client are advised to upgrade to this updated package, which adds this enhancement.

B.88. spice-xpi

B.88.1. RHSA-2011:0426 – Moderate: spice-xpi security update

An updated spice-xpi package that fixes two security issues 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 gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol used in Red Hat Enterprise Linux for viewing virtualized guests running on the Kernel-based Virtual Machine (KVM) hypervisor, or on Red Hat Enterprise Virtualization Hypervisor.

CVE-2011-1179

The spice-xpi package provides a plug-in that allows the SPICE client to run from within Mozilla Firefox.

An uninitialized pointer use flaw was found in the SPICE Firefox plug-in. If a user were tricked into visiting a malicious web page with Firefox while the SPICE plug-in was enabled, it could cause Firefox to crash or, possibly, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-0012

It was found that the SPICE Firefox plug-in used a predictable name for one of its log files. A local attacker could use this flaw to conduct a symbolic link attack, allowing them to overwrite arbitrary files accessible to the user running Firefox.

Users of spice-xpi should upgrade to this updated package, which contains backported patches to correct these issues. After installing the update, Firefox must be restarted for the changes to take effect.

B.89. sssd

B.89.1. RHBA-2010:0971 – sssd bug fix update

Updated sssd packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

The System Security Services Daemon (SSSD) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.

Bug Fixes

BZ#658374

During an upgrade of the sssd package, the package manager restarts the sssd service to ensure the running instance is properly replaced with the newer version. However, prior to this update, a race condition could occur upon the service shutdown, causing the parent process not to wait for its children to terminate. When this happened, these running sub-processes may have prevented sssd from starting again. With this update, the sssd service has been corrected to wait for the children processes to terminate, so that it can be restarted as expected.

BZ#660585

On 32-bit architectures, running the "getent passwd" command on a username with a very large user or group identifier (that is, UID or GID greater than 2147483647) resulted in an empty output. With this update, the underlying source code has been modified to address this issue, and the getent command now returns the expected output.

BZ#660592

Previously, shutting down the sssd service (either by using the "service sssd stop" command, or with the SIGTERM signal) could cause the service to stop responding. This error has been fixed, and sssd no longer fails to shut down.

All users of sssd are advised to upgrade to these updated packages, which resolve these issues.

B.89.2. RHBA-2010:0852 – sssd bug fix update

An updated sssd package that addresses group assignment and multilib issues is now available for Red Hat Enterprise Linux 6.

The System Security Services Daemon (SSSD) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.

Bug Fixes

BZ#637070

Previously, Kerberos applications running on the secondary architecture of a multilib platform (e.g. i686 on x86_64) would not be able to identify the Kerberos server for authentication. With this update, the Kerberos locator plugin is located in the sssd-client package to allow installation of both the 32-bit and 64-bit versions on 64-bit systems.

BZ#642412

Previously, users would not always be assigned to all initgroups for which they were a member in LDAP. This could cause several issues related to group-based permissions. With this update, the initgroups() call always returns all groups for the specified user.

BZ#649312

Previously, SSSD could remove legitimate groups that were only identified as a user's primary group when the cache cleanup routine ran. This could cause issues with group-based access control permissions such as access.conf and sudoers. With this update, SSSD checks also whether there are users who have this group as their primary group ID.

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

B.90. subversion

B.90.1. RHSA-2011:0258 – Moderate: subversion security update

Updated subversion packages that fix three 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Subversion (SVN) is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. The mod_dav_svn module is used with the Apache HTTP Server to allow access to Subversion repositories via HTTP.

CVE-2010-3315

An access restriction bypass flaw was found in the mod_dav_svn module. If the SVNPathAuthz directive was set to "short_circuit", certain access rules were not enforced, possibly allowing sensitive repository data to be leaked to remote users. Note that SVNPathAuthz is set to "On" by default.

CVE-2010-4644

A server-side memory leak was found in the Subversion server. If a malicious, remote user performed "svn blame" or "svn log" operations on certain repository files, it could cause the Subversion server to consume a large amount of system memory.

CVE-2010-4539

A NULL pointer dereference flaw was found in the way the mod_dav_svn module processed certain requests. If a malicious, remote user issued a certain type of request to display a collection of Subversion repositories on a host that has the SVNListParentPath directive enabled, it could cause the httpd process serving the request to crash. Note that SVNListParentPath is not enabled by default.

All Subversion users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the Subversion server must be restarted for the update to take effect: restart httpd if you are using mod_dav_svn, or restart svnserve if it is used.

B.90.2. RHSA-2011:0328 – Moderate: subversion security update

Updated subversion 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.

Subversion (SVN) is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. The mod_dav_svn module is used with the Apache HTTP Server to allow access to Subversion repositories via HTTP.

CVE-2011-0715

A NULL pointer dereference flaw was found in the way the mod_dav_svn module processed certain requests to lock working copy paths in a repository. A remote attacker could issue a lock request that could cause the httpd process serving the request to crash.

Red Hat would like to thank Hyrum Wright of the Apache Subversion project for reporting this issue. Upstream acknowledges Philip Martin, WANdisco, Inc. as the original reporter.

All Subversion users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, you must restart the httpd daemon, if you are using mod_dav_svn, for the update to take effect.

B.91. sysstat

B.91.1. RHBA-2010:0912 – sysstat bug fix update

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

The sysstat package provides the sar and iostat commands. These commands enable system monitoring of disk, network, and other I/O activity.

Bug Fix

BZ#650125

Due to recent changes in the /proc/interrupts format, running the "mpstat -I ALL" command did not produce the correct output. With this update, the mpstat utility has been updated to recognize the new format, and running the above command now works as expected.

BZ#651813

On a system with a running KVM virtual machine and under very special circumstances, the mpstat utility may have produced an output that contained incorrect values. This error no longer occurs, and the mpstat utility now always produces the correct output.

All users of sysstat are advised to upgrade to this updated package, which resolves these issues.

B.92. system-config-firewall

B.92.1. RHBA-2010:0942 – system-config-firewall bug fix update

Updated system-config-firewall packages that fix a bug are now available for Red Hat Enterprise Linux 6.

system-config-firewall is a graphical user interface for basic firewall setup.

Bug Fix

BZ#636110

Prior to this update, certain dialog windows in the Tamil translation of the Firewall Configuration utility contained untranslated strings. With this update, the remaining strings have been translated into the Tamil language, so that dialog windows no longer contain English texts.

Users of system-config-firewall are advised to upgrade to these updated packages, which resolve this issue.

B.93. system-config-users

B.93.1. RHBA-2011:0221 – system-config-users bug fix update

An updated system-config-users package that fixes a bug that caused new user creation to fail in some circumstances is now available.

system-config-users is a graphical utility for administrating users and groups. It depends on the libuser library.

Bug Fix

BZ#672822

When creating users, or more specifically their home directories, system-config-users relied on the access() system call to check if a directory was writable (and, consequently, whether a new home directory could be created in the requested location).

The access() system call returns reliable information for POSIX-compliant (or mostly POSIX-compliant) file-systems only. In some cases, therefore, relying on the information returned by access() could result in user creation failing.

If, for example, system-config-users was directed to create a user with a home folder in a directory managed by an auto-mounter (such as /net), access() returned inaccurate information and user creation subsequently failed.

With this update, system-config-users no longer relies on access(), or other operating system functions, in such cases: it now attempts to create the home directory and checks whether it has succeeded in doing so.

As well, if the chosen location is not writable, system-config-users returns an alert to this effect and requests 'a writable location' be chosen rather than simply writing errors to the terminal and failing.

Users should upgrade to this updated package, which resolves this issue.

B.94. systemtap

B.94.1. RHSA-2010:0894 – Important: systemtap security update

Updated systemtap 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.

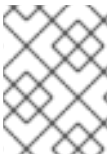
SystemTap is an instrumentation system for systems running the Linux kernel, version 2.6. Developers can write scripts to collect data on the operation of the system. staprun, the SystemTap runtime tool, is used for managing SystemTap kernel modules (for example, loading them).

CVE-2010-4170

It was discovered that staprun did not properly sanitize the environment before executing the modprobe command to load an additional kernel module. A local, unprivileged user could use this flaw to escalate their privileges.

CVE-2010-4171

It was discovered that staprun did not check if the module to be unloaded was previously loaded by SystemTap. A local, unprivileged user could use this flaw to unload an arbitrary kernel module that was not in use.



NOTE

Note: After installing this update, users already in the stapdev group must be added to the stapusr group in order to be able to run the staprun tool.

Red Hat would like to thank Tavis Ormandy for reporting these issues.

SystemTap users should upgrade to these updated packages, which contain backported patches to correct these issues.

B.95. tdb-tools

B.95.1. RHEA-2011:1430 – new packages: tdb-tools

New tdb-tools packages are now available for Red Hat Enterprise Linux 6.

The tdb-tools packages contain tools that can be used to backup and manage tdb files created by Samba.

BZ#717689

This enhancement update adds the tdb-tools packages to Red Hat Enterprise Linux 6.

All tdb users who wish to backup and manage tdb files are advised to install these new packages.

B.96. thunderbird

B.96.1. RHSA-2010:0896 – Moderate: thunderbird security update

An updated thunderbird package that fixes several security issues 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 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.

CVE-2010-3765

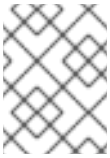
A race condition flaw was found in the way Thunderbird handled Document Object Model (DOM) element properties. An HTML mail message containing malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2010-3175, CVE-2010-3176, CVE-2010-3179, CVE-2010-3180, CVE-2010-3183

Several flaws were found in the processing of malformed HTML mail 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-2010-3178

A same-origin policy bypass flaw was found in Thunderbird. Remote HTML content could steal private data from different remote HTML content Thunderbird had loaded.



NOTE

Note that JavaScript support is disabled by default in Thunderbird. The above issues are not exploitable unless JavaScript is enabled.

CVE-2010-3182

A flaw was found in the script that launches Thunderbird. The LD_LIBRARY_PATH variable was appending a "." character, which could allow a local attacker to execute arbitrary code with the privileges of a different user running Thunderbird, if that user ran Thunderbird from within an attacker-controlled directory.

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

B.96.2. RHSA-2010:0969 – Moderate: thunderbird security update

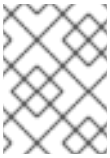
An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which 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.

CVE-2010-3776, CVE-2010-3777

Several flaws were found in the processing of malformed HTML content. Malicious HTML content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.



NOTE

Note that JavaScript support is disabled in Thunderbird for mail messages. The above issues are believed to not be exploitable without JavaScript.

CVE-2010-3768

This update adds support for the Sanitiser for OpenType (OTS) library to Thunderbird. This library helps prevent potential exploits in malformed OpenType fonts by verifying the font file prior to use.

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

B.96.3. RHSA-2011:0311 – Critical: thunderbird security update

An updated thunderbird package that fixes several 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 scores, 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.

CVE-2010-1585, CVE-2011-0053, CVE-2011-0062

Several flaws were found in the processing of malformed HTML content. Malicious HTML content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2011-0061

A flaw was found in the way Thunderbird handled malformed JPEG images. An HTML mail message containing a malicious JPEG image could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

B.96.4. RHSA-2011:0374 – Important: thunderbird security and bug fix update

An updated thunderbird package that fixes one security issue and one bug is 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.

Mozilla Thunderbird is a standalone mail and newsgroup client.

This erratum blacklists a small number of HTTPS certificates. (BZ#689430)

Bug Fix

BZ#683076

The RHSA-2011:0312 and RHSA-2011:0311 updates introduced a regression, preventing some Java content and plug-ins written in Java from loading. With this update, the Java content and plug-ins work as expected.

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

B.96.5. RHSA-2011:0475 — Critical: thunderbird security update

An updated thunderbird package that fixes several 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 scores, 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.

CVE-2011-0080, CVE-2011-0081

Several flaws were found in the processing of malformed HTML content. An HTML mail message containing malicious content could possibly lead to arbitrary code execution with the privileges of the user running Thunderbird.

CVE-2011-0078

An arbitrary memory write flaw was found in the way Thunderbird handled out-of-memory conditions. If all memory was consumed when a user viewed a malicious HTML mail message, it could possibly lead to arbitrary code execution with the privileges of the user running Thunderbird.

CVE-2011-0077

An integer overflow flaw was found in the way Thunderbird handled the HTML frameset tag. An HTML mail message with a frameset tag containing large values for the "rows" and "cols" attributes could trigger this flaw, possibly leading to arbitrary code execution with the privileges of the user running Thunderbird.

CVE-2011-0075

A flaw was found in the way Thunderbird handled the HTML iframe tag. An HTML mail message with an iframe tag containing a specially-crafted source address could trigger this flaw, possibly leading to arbitrary code execution with the privileges of the user running Thunderbird.

CVE-2011-0074

A flaw was found in the way Thunderbird displayed multiple marquee elements. A malformed HTML mail message could cause Thunderbird to execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2011-0073

A flaw was found in the way Thunderbird handled the nsTreeSelection element. Malformed content could cause Thunderbird to execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2011-0071

A directory traversal flaw was found in the Thunderbird resource:// protocol handler. Malicious content could cause Thunderbird to access arbitrary files accessible to the user running Thunderbird.

CVE-2011-0070

A double free flaw was found in the way Thunderbird handled "application/http-index-format" documents. A malformed HTTP response could cause Thunderbird to execute arbitrary code with the privileges of the user running Thunderbird.

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

B.97. tomcat6

B.97.1. RHSA-2011:0335 – Important: tomcat6 security and bug fix update

Updated tomcat6 packages that fix two security issues and one bug 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.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

CVE-2010-4476

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Tomcat to hang via a specially-crafted HTTP request.

CVE-2011-0534

A flaw was found in the Tomcat NIO (Non-Blocking I/O) connector. A remote attacker could use this flaw to cause a denial of service (out-of-memory condition) via a specially-crafted request containing a large NIO buffer size request value.

Bug Fix

BZ#676922

A bug in the "tomcat6" init script prevented additional Tomcat instances from starting. As well, running "service tomcat6 start" caused configuration options applied from "/etc/sysconfig/tomcat6" to be overwritten with those from "/etc/tomcat6/tomcat6.conf". With this update, multiple instances of Tomcat run as expected.

Users of Tomcat should upgrade to these updated packages, which contain backported patches to correct these issues. Tomcat must be restarted for this update to take effect.

B.98. tuned

B.98.1. RHBA-2010:0847 – tuned bug fix update

Updated tuned packages that fix profiles performing I/O scheduler changes.

Tuned is a utility for tuning system performance and power-consumption. Various profiles are available.

Bug Fix

BZ#638975

Prior to this update, I/O scheduler changes were not applied to device mapper (dm) devices, which affected the enterprise-storage, latency-performance and throughput-performance profiles. This error has been fixed, device mapper devices have been added to the "ELEVATOR_TUNE_DEVS" list, and I/O scheduler changes are now applied to all devices as expected.

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

B.99. upstart

B.99.1. RHBA-2010:0848 – upstart bug fix update

An updated upstart package that fixes a bug in utmp table updating is now available.

Upstart is an event-based replacement for the /sbin/init daemon, which handles starting of tasks and services during boot, stopping them during shut down, and supervising them while the system is running.

Bug Fix

BZ#636487

When a mingetty session is terminated, the relevant entry in the utmp table is now correctly set to "DEAD_PROCESS".

All users are advised to upgrade to this updated package, which resolves this issue. Note that after installing this update, a system reboot is required for the above changes to take effect.

B.100. util-linux-ng

B.100.1. RHBA-2011:0201 – util-linux-ng bug fix update

Updated util-linux-ng packages that fix a bug in the mount utility are now available for Red Hat Enterprise Linux 6.

The util-linux-ng package contains a large variety of low-level system utilities that are necessary for a Linux system to function.

Bug Fix

BZ#659612

To address problems with iSCSI root devices not being checked with the fsck utility, Red Hat Enterprise Linux 5.2 introduced the "_rnetdev" mount option. However, this functionality was missing in the package for Red Hat Enterprise Linux 6. With this update, the mount utility has been updated to support this option.

Users of util-linux-ng should upgrade to these updated packages, which resolve this issue.

B.101. vsftpd

B.101.1. RHSA-2011:0337 – Important: vsftpd security update

An updated vsftpd package that fixes one security issue is 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.

vsftpd (Very Secure File Transfer Protocol (FTP) daemon) is a secure FTP server for Linux, UNIX, and similar operating systems.

CVE-2011-0762

A flaw was discovered in the way vsftpd processed file name patterns. An FTP user could use this flaw to cause the vsftpd process to use an excessive amount of CPU time, when processing a request with a specially-crafted file name pattern.

All vsftpd users should upgrade to this updated package, which contains a backported patch to correct this issue. The vsftpd daemon must be restarted for this update to take effect.

B.102. webkitgtk

B.102.1. RHSA-2011:0177 – Moderate: webkitgtk security update

Updated webkitgtk 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 scores, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

WebKitGTK+ is the port of the portable web rendering engine WebKit to the GTK+ platform.

CVE-2010-1782, CVE-2010-1783, CVE-2010-1784, CVE-2010-1785, CVE-2010-1787, CVE-2010-1788, CVE-2010-1790, CVE-2010-1792, CVE-2010-1807, CVE-2010-1814, CVE-2010-3114, CVE-2010-3116, CVE-2010-3119, CVE-2010-3255, CVE-2010-3812, CVE-2010-4198

Multiple memory corruption flaws were found in WebKit. Malicious web content could cause an application using WebKitGTK+ to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2010-1780, CVE-2010-1786, CVE-2010-1793, CVE-2010-1812, CVE-2010-1815, CVE-2010-3113, CVE-2010-3257, CVE-2010-4197, CVE-2010-4204

Multiple use-after-free flaws were found in WebKit. Malicious web content could cause an application using WebKitGTK+ to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2010-4206, CVE-2010-4577

Two array index errors, leading to out-of-bounds memory reads, were found in WebKit. Malicious web content could cause an application using WebKitGTK+ to crash.

CVE-2010-3115

A flaw in WebKit could allow malicious web content to trick a user into thinking they are visiting the site reported by the location bar, when the page is actually content controlled by an attacker.

CVE-2010-3259

It was found that WebKit did not correctly restrict read access to images created from the "canvas" element. Malicious web content could allow a remote attacker to bypass the same-origin policy and potentially access sensitive image data.

CVE-2010-3813

A flaw was found in the way WebKit handled DNS prefetching. Even when it was disabled, web content containing certain "link" elements could cause WebKitGTK+ to perform DNS prefetching.

Users of WebKitGTK+ should upgrade to these updated packages, which contain WebKitGTK+ version 1.2.6, and resolve these issues. All running applications that use WebKitGTK+ must be restarted for this update to take effect.

B.103. wireshark

B.103.1. RHSA-2010:0924 – Moderate: wireshark security update

Updated wireshark 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 scores, 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.

CVE-2010-4300

A heap-based buffer overflow flaw was found in the Wireshark Local Download Sharing Service (LDSS) dissector. 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-2010-3445

A denial of service flaw was 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 Wireshark version 1.2.13, and resolve these issues. All running instances of Wireshark must be restarted for the update to take effect.

B.103.2. RHSA-2011:0013 – Moderate: wireshark security update

Updated wireshark 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 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.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

CVE-2010-4538

An array index error, leading to a stack-based buffer overflow, was found in the Wireshark ENTTEC dissector. 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.

Users of Wireshark should upgrade to these updated packages, which contain a backported patch to correct this issue. All running instances of Wireshark must be restarted for the update to take effect.

B.103.3. RHSA-2011:0369 – Moderate: wireshark security update

Updated wireshark 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 scores, 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.

CVE-2011-0444

A heap-based buffer overflow flaw was found in the Wireshark MAC-LTE dissector. 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-2011-0713

A heap-based buffer overflow flaw was found in the way Wireshark processed signaling traces generated by the Gammu utility on Nokia DCT3 phones running in Netmonitor mode. If Wireshark opened a specially-crafted capture file, it could crash or, possibly, execute arbitrary code as the user running Wireshark.

CVE-2011-0538, CVE-2011-1139, CVE-2011-1140, CVE-2011-1141

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 Wireshark version 1.2.15, and resolve these issues. All running instances of Wireshark must be restarted for the update to take effect.

B.104. xguest

B.104.1. RHBA-2010:0853 – xguest bug fix update

An updated xguest package that fixes a bug is now available.

The xguest package sets up the xguest user which can be used as a temporary account to switch to or as a kiosk user account. These accounts are disabled unless SELinux is in enforcing mode.

Bug Fix

BZ#641811

Previously, xguest installed its 'sabayon' profile file in the wrong directory. This would cause packagekit and seapplet to be started by default for the xguest user. With this update, the 'sabayon' profile file is installed in the correct directory.

All users of xguest are advised to upgrade to this updated package, which resolves this issue.

B.105. xorg-x11-drv-qxl

B.105.1. RHBA-2010:0917 – xorg-x11-drv-qxl bug fix update

An updated xorg-x11-drv-qxl package that fixes various bugs is now available.

xorg-x11-qxl-drv is 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 KVM and QEMU, using the SPICE protocol.

This updated xorg-x11-drv-qxl package includes fixes for the following bugs:

BZ#648933

When using the xql driver, only a limited number of resolution choices were available for use inside the guest, none of which exceeded 1024x768 in size unless the xorg.conf configuration file was (first created, and then) manually edited. This update ensures that larger resolutions are available for guests with appropriate hardware without needing to manually change xorg.conf.

BZ#648935

When using the qxl driver, after connecting to a virtual guest over the SPICE protocol and logging into a desktop session from the GDM display manager, attempting to switch to a virtual console using a key combination caused the X server to crash, and GDM to respawn. This update fixes this issue so that, in the aforementioned situation, switching to a virtual console and back to the graphical desktop works as expected.

All users of KVM-based virtualization are advised to upgrade to this updated package, which fixes these issues.

B.106. xorg-x11-drv-wacom and wacomcpl

B.106.1. RHBA-2011:0341 – xorg-x11-drv-wacom and wacomcpl bug fix update

Updated xorg-x11-drv-wacom and wacomcpl packages that resolve several issues 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.

These updated xorg-x11-drv-wacom and wacomcpl packages provide fixes for the following bugs:

BZ#675908

Changing the screen mapping caused the wacompl GUI to become unresponsive. With this update, changing the screen mapping works as expected.

BZ#642915

Attempting to calibrate a device could have failed with an error message. With this update, calibration now succeeds.

All users of xorg-x11-drv-wacom and wacomcpl are advised to upgrade to these updated packages, which resolve these issues.

B.107. xorg-x11-server

B.107.1. RHBA-2011:0340 – xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix a bug are now available for Red Hat Enterprise Linux 6.

X.Org X11 is an open source implementation of the X Window System. It provides the basic low level functionality upon which full fledged graphical user interfaces such as GNOME and KDE are designed.

Bug Fix

BZ#668514

Prior to this update, when the X Window System was unable to detect a monitor and obtain valid extended display identification data (EDID), it set the default resolution limit to 800x600. Consequent to this, users of the "mga" driver for Matrox video cards were unable to select a screen resolution higher than 800x600. This update increases the default limit to 1024x768, allowing users of Matrox video cards to select this resolution as expected.

All users of xorg-x11-server are advised to upgrade to these updated packages, which resolve this issue.

B.108. xorg-x11-server-utils

B.108.1. RHSA-2011:0433 – Moderate: xorg-x11-server-utils security update

An updated xorg-x11-server-utils package that fixes one security issue is 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 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.

CVE-2011-0465

A flaw was found in the X.Org X server resource database utility, xrdb. Certain variables were not properly sanitized during the launch of a user's graphical session, which could possibly allow a remote attacker to execute arbitrary code with root privileges, if they were able to make the display manager execute xrdb with a specially-crafted X client hostname. For example, by configuring the hostname on the target system via a crafted DHCP reply, or by using the X Display Manager Control Protocol (XDMCP) to connect to that system from a host that has a special DNS name.

Red Hat would like to thank Matthieu Herrb for reporting this issue. Upstream acknowledges Sebastian Krahmer of the SuSE Security Team as the original reporter.

Users of xorg-x11-server-utils should upgrade to this updated package, which contains a backported patch to resolve this issue. All running X.Org server instances must be restarted for this update to take effect.

B.108.2. RHBA-2011:0453 – xorg-x11-server-utils bug fix update

An updated xorg-x11-server-utils package that fixes one bug is 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.

Bug Fix

BZ#696310

A previous advisory, the RHSA-2011:0433 xorg-x11-server-utils security update, applied a backported patch to fix a flaw in the X server resource database utility, xrdb. While this patch resolved the security issue, it also introduced an error in the macro expansion mechanism. Consequent to this, an attempt to run the xrdb utility could fail with the following messages written to standard error:

```
sh: -c: line 0: unexpected EOF while looking for matching `"'
sh: -c: line 1: syntax error: unexpected end of file
```

With this update, the underlying source code has been adapted to correct the macro expansion mechanism, and the xrdb utility now works as expected.

All users of xorg-x11-server-utils are advised to upgrade to this updated package, which fixes this bug. Note that all running instances of the X.Org server must be restarted for this update to take effect.

B.109. yaboot

B.109.1. RHBA-2010:0854 – yaboot bug fix update

An updated yaboot package that fixes a bug is now available.

The yaboot package is a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

Bug Fix

BZ#642694

Previously, yaboot netboot failed to operate in an environment where the gateway is not same as the 'tftp' server, even though the 'tftp' server is on the same subnet. This issue was caused by yaboot's inability to check whether an IP address is valid. With this update, an IP address validity check has been added that resolves this issue.

All users of yaboot are advised to upgrade to this updated package, which resolves this issue.

B.110. yum

B.110.1. RHBA-2010:0846 – yum bug fix update

An updated yum package that fixes various bugs is now available.

Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically, prompting the user for permission as necessary.

Bug Fixes

BZ#634974

Previously, yum treated packages that provide kernel-modules as install-only packages. With this update, the install-only option has been removed.

BZ#637086

Previously, the "/var/cache/yum/" directory kept accumulating multiple '.sqlite' files and never cleaned them out. With this update, the '.sqlite' are automatically cleaned up.

All users of yum are advised to upgrade to this updated package, which resolves these issues.

B.111. yum-rhn-plugin and rhn-client-tools

B.111.1. RHEA-2010:0949 – yum-rhn-plugin and rhn-client-tools enhancement update

Updated yum-rhn-plugin and rhn-client-tools packages that add an enhancement are now available for Red Hat Enterprise Linux 6.

Red Hat Network Client Tools provide programs and libraries that allow a system to receive software updates from Red Hat Network (RHN). yum-rhn-plugin allows yum to access a Red Hat Network server for software updates.

Enhancement

BZ#649435

These packages have been updated to support the Red Hat Network Satellite Server Maintenance Window, allowing a user to download scheduled packages and errata before the start of the maintenance window.

Users of rhn-client-tools and yum-rhn-plugin are advised to upgrade to these updated packages, which add this enhancement. Note that this feature is disabled by default. For information on how to enable it, refer to https://access.redhat.com/site/solutions/42227.

C. REVISION HISTORY

Revision 1-6.12 **Fri Feb 27 2015** **Laura Bailey**
Rebuild for sort order.

Revision 1-6.10 **Wed Jan 22 2014** **Eliška Slobodová**
Added the missing eCryptfs Technology Preview.

Revision 1-6.8 **Mon Jun 17 2013** **Eliška Slobodová**
Fixed broken links and links pointing to the old Product Documentation site.

Revision 1-6.7 **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* appendix of this book.

Revision 1-5 **Thu May 19 2011** **Ryan Lerch**
Removed Package Manifest data. Provided link to new Package Manifest document

Revision 1-5 **Tue Nov 16 2010** **Ryan Lerch**
Fixed invalid links

Revision 1-0 **Wed Nov 10 2010** **Ryan Lerch**
Initial Release of the Technical Notes