Red Hat Enterprise Linux 6

6.1 Technical Notes

Technical Release Documentation

Edition 1

Last Updated: 2017-10-24

Red Hat Enterprise Linux 6 6.1 Technical Notes

Technical Release Documentation
Edition 1

Red Hat Engineering Content Services

Legal Notice

Abstract

The Red Hat Enterprise Linux 6.1 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications between Red Hat Enterprise Linux 6.0 and minor release Red Hat Enterprise Linux 6.1.

Table of Contents

The Red Hat Enterprise Linux 6.1 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications between Red Hat Enterprise Linux 6.0 and minor release Red Hat Enterprise Linux 6.1.

For system administrators and others planning Red Hat Enterprise Linux 6.1 upgrades and deployments, the Technical Notes provide a single, organized record of the bugs fixed in, features added to, and Technology Previews included with this new release of Red Hat Enterprise Linux.

For auditors and compliance officers, the Red Hat Enterprise Linux 6.1 Technical Notes provide a single, organized source for change tracking and compliance testing.

For every user, the Red Hat Enterprise Linux 6.1 Technical Notes provide details of what has changed in this new release.

NOTE

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

1. 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.

1.1. 389-ds-base

1.1.1. RHBA-2011:0824 — 389-ds-base bug fix update

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

389 Directory Server is an LDAPv3 compliant server. The base package includes the LDAP server and command-line utilities for server administration.

Bug Fixes

BZ#701554

Password changes did not replicate because the method used to pass the changes to consumer servers was rejected on the consumer. This issue has been corrected, and password changes now replicate as expected.

BZ#701556

Values could be lost when group memberships were synchronized between 389 Directory Server and Active Directory with the Windows Sync feature. The synchronization and modify operations have been altered to prevent this issue, allowing group updates to synchronize with Active Directory.

BZ#701558

The ldclt command-line testing tool crashed during LDAP ADD operations because an LDAP attribute was not set correctly, preventing the creation of entries that did not already exist. This update allows the LDAP ADD to proceed correctly.

BZ#701559

The server crashed if a long running task was started using the cn=tasks,cn=config interface and then the server was shut down before the task completed. This update prevents the server from crashing, but does not gracefully terminate the task, which can leave the server database in an inconsistent state. For example, the fixup-memberof.pl script invokes a tasks to fix up the memberOf attribute in group member entries. If the server is shut down before the task can complete, some entries may not have the correct memberOf values. Users should ensure that tasks are complete before shutting down the server to avoid inconsistency.

BZ#701560

When using the Entry USN feature, deleting an entry caused a memory leak via the entryusn attribute. This update fixes the memory leak.

All 389-ds-base users are advised to upgrade to these updated packages, which addresses these issues.

1.2. abrt

1.2.1. RHBA-2011:0619 — abrt bug fix update

Updated abrt packages that resolve several issues are now available for Red Hat Enterprise Linux 6.

The abrt package provides the Automatic Bug Reporting Tool.

The abrt package has been upgraded to upstream version 1.1.16, which provides a number of bug fixes and enhancements over the previous version. (BZ#650975)

Bug Fixes

BZ#576866

Prior to this update, the ABRT GUI did not warn the user when it could not connect to the Gnome keyring daemon (that is, could not save any of the user's settings). With this update, a warning message is displayed in such a case.

BZ#614486

The previous version of ABRT did not properly restore the core_pattern parameter (which is used to specify a coredump file pattern name) if it was too long. This update restores the core_pattern parameter to its previous value when the abrt daemon is stopped.

BZ#623142

If the TAINT_HARDWARE_UNSUPPORTED flag, which detecs hardware not officially supported by Red Hat, is set (in the /proc/sys/kernel/taint file), ABRT indicates that the flag is set in the created crash report.

BZ#649309

The abrt-addon-ccpp plugin crashed due to a segmentation fault if the /proc/[PID]/ directory did not exist. With this update, ABRT no longer crashes in case the /proc/[PID]/ directory does not exist.

BZ#665405

Content from various files in the /var/log/ directory is now included in the creation of an sosreport (which is created via the abrt-plugin-sosreport plugin).

BZ#666267

Prior to this update, the "Help" button in the ABRT GUI displayed the "About" window. With this update, a proper help page is displayed.

BZ#668875

Occasionally, ABRT did not send an attached core dump file along with a crash report. This was due to the large size of the core dump file which was consequently rejected by the server which was receiving the crash report. With this update, attachments and their sizes are listed in the crash report, making it easier to detect any problems caused by the large size of the attachments.

BZ#670492

Previously, ABRT was using "Strata-Message:" headers in server responses. However, servers no longer use these headers. With this update, the aforementioned headers are no longer used by ABRT.

BZ#678724

By default, in Red Hat Enterprise Linux 6, ABRT did not enable any reporters, causing environments which do not run an X server to not be notified of any crashes ABRT detected. With this update, the mailx plugin is enabled as the default reporter for every crash and the root user is now notified of any crashes via the root@localhost mailbox.

BZ#694410

The duplicate hash of a crash was computed from the package NVR (Name, Version, Release), path of the executable and the backtrace hash. This caused the hash to be different for the same bug which occurred in two versions of the same package. With this update, the component name and the backtrace hash are used when computing the duplicate hash.

All users of abrt are advised to upgrade to these updated packages, which resolve these issues.

1.3. acroread

1.3.1. RHBA-2011:0813 — acroread bug fix update

Updated acroread packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

Adobe Reader allows users to view and print documents in Portable Document Format (PDF).

Bug Fix

BZ#680202

With a recent update, the OpenLDAP libraries have been moved to different directory. This update changes the way Adobe Reader links to these libraries.

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

1.4. anaconda

1.4.1. RHBA-2011:0530 — anaconda bug fix and enhancement update

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

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

Bug Fixes

BZ#593642

Auto-partitioning no longer clears immutable partitions.

BZ#593984

Anaconda no longer creates a new EFI system partition when one is not needed.

BZ#601862, BZ#614812

Anaconda now properly detects ext2's dirty/clean states.

BZ#609570

Anaconda no longer forgets IP method selection in the loader when returning to a previous menu.

BZ#611825

The "Proxy password" field in stage 2 now correctly displays asterisks instead of plain text.

BZ#612476

Text mode now allows IPv6 configuration.

BZ#626025

Anaconda no longer displays free regions of less than 1MB in extended partitions.

BZ#671017

Anaconda no longer loses focus on certain screens.

BZ#634655

".treeinfo" files are now properly fetched over a proxy.

BZ#635201

Anaconda now writes correct NFS (Network File System) repository information into the summary Kickstart file.

BZ#638734

The /boot/ directory can now reside on an ext4 partition.

BZ#654360

Anaconda no longer fails to detect a disk if its size exceeds 1TB.

BZ#678028

Anaconda is once again able to detect the file system on a previously-created RAID device.

BZ#692350

Anaconda now generates the correct, FIPS-enabled initramfs (initial RAM file system) when the kernel option "fips=1" is provided on the kernel command line.

BZ#640260

Anaconda incorrectly failed with a traceback when an attempt to unpack a driver disk to a pre-existing root partition.

BZ#676854

Fingerprint authentication has been disabled on IBM System z because it is not supported on that platform.

BZ#641324

Static IPv4 configuration is now used when requested in stage 2: Anaconda no longer falls back to using DHCP.

BZ#652874

Anaconda is now able to properly detect an md RAID array with a spare disk.

BZ#636533

Anaconda now correctly reports an error when a network-based certificate is specified in Kickstart with no networking setup.

BZ#621490

A custom value is now properly honored when shrinking a file system.

BZ#702430

The "list-harddrives" command output for CCISS devices is now valid input for Kickstart files.

BZ#683891

Anaconda now selects the new kernel after upgrade.

Enhancements

BZ#442980, BZ#529443

This update adds the cnic, bnx2i, and be2net drivers for better iSCSI support.

BZ#633307, 633319

This update adds drivers for the Emulex 10GbE PCI-E Gen2 and Chelsio T4 10GbE network adapters.

BZ#554874

Algorithms from the SHA-2 hash function family can now be used to encrypt the boot loader password.

BZ#607827

Anaconda now allows a username and password to be entered for iSCSI Discovery sessions.

BZ#354432, 614399

The "rdate", "which", "tty" and "ntpdate" commands have been added to the install image.

BZ#663411

The graphical installer now runs using the full display resolution.

BZ#667122, BZ#599042, BZ#678574

Anaconda now features improved SSL certificate-handling.

BZ#621349

It is now possible to specify additional packages when using the "@packages --default" Kickstart option.

BZ#618376

On IBM System z, the /boot/ directory can now be placed on an LVM logical volume.

BZ#644535

Anaconda now supports blacklisting to determine which modules can be loaded during installation.

Users are advised to upgrade to this updated anaconda package, which resolves these issues and adds these enhancements.

1.5. apr

1.5.1. RHSA-2011:0844 — Low: 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 low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The 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.

Security Fix

CVE-2011-1928

The fix for CVE-2011-0419 (released via RHSA-2011:0507) introduced an infinite loop flaw in the apr_fnmatch() function when the APR_FNM_PATHNAME matching flag was used. A remote attacker could possibly use this flaw to cause a denial of service on an application using the apr_fnmatch() function.

Note: This problem affected httpd configurations using the "Location" directive with wildcard URLs. The denial of service could have been triggered during normal operation; it did not specifically require a malicious HTTP request.

This update also addresses additional problems introduced by the rewrite of the apr_fnmatch() function, which was necessary to address the CVE-2011-0419 flaw.

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.

1.6. at

1.6.1. RHBA-2011:0016 — at bug fix update

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

At and batch read commands from standard input or from a specified file. At allows you to specify that a command will be run at a particular time. Batch will execute commands when the system load levels drop to a particular level. Both commands use /bin/sh.

Bug Fixes

BZ#589099

Previously, the at daemon (atd) wrongly contained permissions 0755 for atd configuration. With this update, atd has the correct permissions 0644 as have all other such files.

BZ#615104

Previously, the initscript caused the "OK" message to be printed twice. With this update, the initscript behaves as expected and does no longer cause echos of messages.

BZ#630019

Previously, the PIE label was not compiled with -fpie/-fPIE. This update adds a PIE compile option for secure positions independently executable on targets.

All users of at are advised to upgrade to this updated package, which resolves this issue.

1.7. authconfig

1.7.1. RHBA-2011:0595 — authconfig bug fix and enhancement update

Updated authconfig packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

The authconfig package contains a command line utility and a GUI application that can configure a workstation to be a client for certain network user information and authentication schemes and other user information and authentication related options.

The authconfig package has been upgraded to upstream version 6.1.12, which provides a number of bug fixes and enhancements over the previous version. This version also adds new options: "--enableforcelegacy" and "--disableforcelegacy". These options allow the user to use legacy LDAP and Kerberos user identity and authentication modules instead of the SSSD modules. (BZ#655910)

Bug Fixes

BZ#595261

Prior to this update, authconfig unnecessarily restarted the user information and authentication services even though there were no configuration changes that would require the restart. With this update, services are no longer restarted unless explicitly required.

BZ#620475

The authentication configuration utility did not keep the "Require smart card for login" check box set when Kerberos was also enabled. When the check box was checked and the configuration was saved with the "Apply" button, the system would correctly require smart card for login. However, on the subsequent run of the authentication configuration utility the check box would be unchecked again and it was necessary to check it again to keep the option switched on. With this update, the "Require smart card for login" stays checked even after subsequent runs of the authentication configuration utility.

BZ#621632

The authentication configuration tool GUI incorrectly duplicated its window when the "Revert" button was pressed. This update fixes the duplicity problem.

BZ#624159

In some cases, when multiple configuration files with the same configuration settings contained different configuration values for a setting, the configuration files contents were not properly synchronized with authconfig. With this update, the synchronization works as expected.

BZ#639747

The authentication configuration tool GUI allowed to choose user identity and authentication schemes which require packages that are not installed on the system by default. With this update, certain identity and authentication schemes cannot be configured when they are not installed on the system.

BZ#663882

The authconfig textual user interface incorrectly required the nss-pam-ldap package to be installed when the configuration used SSSD for LDAP user identification. With this update, the nss-pam-ldap package is not required in such a case.

BZ#674844

Prior to this update, the authentication configuration tool overwrote the cache_credentials value to "True" in the SSSD configuration file (/etc/sssd/sssd.conf) if the configuration allowed using SSSD for the network user information and authentication services. With this update, the "cache_credentials" parameter is no longer overwritten in the aforementioned case.

BZ#676333

The "system-config-authentication" command crashed when executed in an environment without the X server running. With this update, a proper error message is printed in the aforementioned case.

Users are advised to upgrade to these updated authconfig packages, which resolve these issues and add this enhancement.

1.8. audit

1.8.1. RHBA-2012:0653 — audit bug fix and enhancement update

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

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

The audit packages are have been upgraded to upstream version 2.1. (BZ#584981) This upgrade provides the following bug fixes and enhancements over the previous version:

- autrace now uses the correct syscalls on i386 systems
- Added support for new event types related to virtualization, netfilter, the mmap syscall, key based authentication, and cryptographic session establishment.
- Updated syscall tables for the 2.6.37 kernel.
- Updated sample rules for new syscalls and packages.
- The overflow_action configuration item was added to audisp-remote to allow configurable actions for remote logging queue overflows.
- A new option in the audisp-syslog plug-in to send syslog audit events to local[0-7]

Bug Fixes

BZ#670938

System processes — that is processes with an audit id (auid) of -1 — are logged by the audit subsystem. However, if the ausearch utility was used to locate events where the auid was -1, it would display all events. In this update, under these circumstances, ausearch only returns events with an auid of -1.

BZ#688664

A value of 'syslog' for the 'disk_error_action' parameter in 'auditd.conf' instructs auditd to issue a warning to syslog if an error is encountered when writing audit events to disk. If 'disk_error_action' was set to 'syslog', auditd always attempted to exec() a child process. Consequently, if a disk error was encountered (ie. a disk full error), auditd would attempt to exec() a null child process, and logging would not resume after the disk error was reported to syslog. In this update the child process is not called when the 'syslog' option is used, and logging continues as expected.

BZ#695605

Previously if an audispd plug-in was restarted, the plug-in was not marked as active. Consequently, the remote logging plug-in (audisp-remote) was unable to bind to a privileged port on reconnect because all privileges had been dropped. In these updated packages, audispd plug-ins are marked as active after being restarted, and the audisp-remote plug-in functions as expected.

BZ#697463

Previously, the "autrace -r" command on the IBM System z architecture attempted to audit network syscalls not available on IBM System z. Consequently, an error similar to the following might have been returned:

```
Error inserting audit rule for pid=13163
```

With this update, "autrace -r" is now aware of system calls not available on this architecture, which resolves this issue.

BZ#640948

When an ignore directive was included in an audit.rules configuration file, the auditctl utility became unresponsive when attempting to load those rules. With this update, the issue is resolved.

BZ#647128

Previously, the audit_encode_nv_string() function was not checking if the memory allocation (malloc) it was performing succeeded. Consequently, if the malloc operation encountered an out of memory (OOM) error, audit_encode_nv_string() crashed attempting to reference a NULL pointer. With this update, audit_encode_nv_string() checks if the malloc is successful, which resolves this issue.

BZ#647131

Previously, the man page for the "audit_encode_nv_string" function incorrectly documented the return value type as an "int". The man page for "audit_encode_nv_string" now correctly displays return value type for the "audit_encode_nv_string" function as a "char *"

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

1.9. autofs

1.9.1. RHBA-2012:0753 — autofs bug fix and enhancement update

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

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

Bug Fixes

BZ#629480

When using client certificates with autofs, the certificate DN could not be used in LDAP ACLs. This prevented autofs from authenticating via SASL external. With this update, the SASL EXTERNAL authentication mechanism is used for mapping the certificate DN to an LDAP DN, allowing autofs to support SASL External authentication via TLS.

BZ#616426

The autfs initscript did not implement the functions force-reload and try-restart. Instead, the error try-restart and force-reload service action not supported was given and returned 3. This patch adds these initscript options so that the they are now implement and return appropriate values.

BZ#629359

Debugging output from autofs did not include IP addresses for mounts alongside hostname information which made it difficult to debug issues when using round-robin DNS. This update adds this feature, allowing logging output to show the IP address of a mount, rather than just the host name.

BZ#572608

Previously, automount woke up once per second to check for any scheduled tasks, despite the fact that adding a task triggered a wake up of that thread, which lead to a tight loop which used excessive CPU. This update removes these unnecessary wakeups.

BZ#520844

When an autofs map entry had multiple host names associated with it, there was no way to override the effect of the network proximity. This was a problem when a need existed to be able to rely on selection strictly by weight. With this patch, the server response time is also taken into consideration when selecting a server for the target of the mount. The pseudo option --use-weight-only was added that can only be used with master map entries or with individual map entries in order to provide this. For individual map entries, the option no-use-weight-only can also be used to override the master map option.

BZ#666340

If there were characters that matched isspace() (such as \t and \n) in a passed map entry key and there was no space in the key, these character were not properly preserved, which led to failed or incorrect mounts. This was caused by an incorrect attempt at optimization by using a check to see if a space was present in the passed key and only then processing each character of the key individually, escaping any isspace() characters. This patch adds a check for isspace() characters to the same check for a space, eliminating the problem.

BZ#630954

If the map type was explicitly specified for a map, then the map was not properly updated when a re-read was requested. This was because the map stale flag was incorrectly cleared after the lookup module read the map, instead of at the completion of the update procedure. In this patch, the map stale flag should only be cleared if the map read fails for some reason, otherwise it updates when the refresh is completed.

BZ#650009

Previously, when autofs was restarted with active mounts, due to a possible recursion when mounting multi-mount map entries, autofs would block indefinitely. This was caused by a cache readlock which was held when calling mount_subtree() from parse_mount () in parse_sun.c. This patch fixes remount locking which resolves the issue.

BZ#577099

The master map DN string parsing is quite strict and, previously, autofs could not use an automount LDAP DN using the l (localityName) attribute. This patch adds the allowable attribute 'l', the locality.

BZ#700691

A previous bug fix caused the state queue manager thread to stop processing events, and mounts expired and then stopped. This was caused when the state queue task manager transferred an automount point pending task to its task queue for execution. The state queue was then mistakenly being seen as empty when the completing task was the only task in the state queue. This patch adds a check to allow the queue manager thread to continue, resolving the issue.

BZ#700697

The autofs gave a segmentation fault on the next null cache look up in the auto.master file. This was due to a regression issue, where a function to clean the null map entry cache, added to avoid a race when re-reading the master map, mistakenly failed to clear the hash bracket array entries. This patch sets the hash bracket array entries to NULL, resolving the issue.

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

1.10. avahi

1.10.1. RHSA-2011:0779 — Moderate: avahi security and bug fix update

Updated avahi 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.

Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zero Configuration Networking. It facilitates service discovery on a local network. Avahi and Avahi-aware applications allow you to plug your computer into a network and, with no configuration, view other people to chat with, view printers to print to, and find shared files on other computers.

Security Fix

CVE-2011-1002

A flaw was found in the way the Avahi daemon (avahi-daemon) processed Multicast DNS (mDNS) packets with an empty payload. An attacker on the local network could use this flaw to cause avahi-daemon on a target system to enter an infinite loop via an empty mDNS UDP packet.

Bug Fix

BZ#629954, BZ#684276

Previously, the avahi packages in Red Hat Enterprise Linux 6 were not compiled with standard RPM CFLAGS; therefore, the Stack Protector and Fortify Source protections were not enabled, and the debuginfo packages did not contain the information required for debugging. This update corrects this issue by using proper CFLAGS when compiling the packages.

All users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. After installing the update, avahi-daemon will be restarted automatically.

1.11. bash

1.11.1. RHBA-2011:0689 — bash bug fix update

Updated bash packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

Bash (Bourne-again shell) is the default shell for Red Hat Enterprise Linux.

Bug Fixes

BZ#618289

When using arithmetic evaluation on an associative array with integer values, an attempt to provide an invalid subscript caused Bash to terminate unexpectedly with a segmentation fault. This update applies a patch that corrects this error, and providing an invalid subscript no longer causes the bash interpreter to crash.

BZ#664468

Prior to this update, the Bash interpreter reported broken pipe errors for both external and built-in commands. Since these errors are only relevant for external commands, this update adapts the underlying source code to suppress the broken pipe error messages for built-in commands. As a result, only relevant messages are now presented to user.

BZ#619704

Previous version of the bash(1) manual page did not provide a clear description of the "break", "continue", and "suspend" built-in commands. This update corrects this error, and extends the manual page to provide accurate and complete descriptions of these commands.

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

1.12. bfa-firmware

1.12.1. RHBA-2011:0593 — bfa-firmware bug fix and enhancement update

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

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

The bfa-firmware package has been upgraded to upstream version 2.3.2.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#617017)

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

1.13. bind

1.13.1. RHSA-2011:0845 — Important: bind security update

Updated bind and bind97 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 Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Security fix

CVE-2011-1910

An off-by-one flaw was found in the way BIND processed negative responses with large resource record sets (RRSets). An attacker able to send recursive queries to a BIND server that is configured as a caching resolver could use this flaw to cause named to exit with an assertion failure.

All BIND users are advised to upgrade to these updated packages, which resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

1.13.2. RHSA-2011:0926 — Important: bind security update

Updated bind and bind97 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 Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Security Fix

CVE-2011-2464

A flaw was discovered in the way BIND handled certain DNS requests. A remote attacker could use this flaw to send a specially-crafted DNS request packet to BIND, causing it to exit unexpectedly due to a failed assertion.

Users of bind97 on Red Hat Enterprise Linux 5, and bind on Red Hat Enterprise Linux 6, are advised to upgrade to these updated packages, which resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

1.13.3. RHSA-2011:1458 — Important: bind security update

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

Security Fix

CVE-2011-4313

A flaw was discovered in the way BIND handled certain DNS queries, which caused it to cache an invalid record. A remote attacker could use this flaw to send repeated queries for this invalid record, causing the resolvers to exit unexpectedly due to a failed assertion.

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

1.13.4. RHBA-2011:0541 — bind bug fix and enhancement update

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

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 applications use when interfacing with DNS), and tools for verifying that the DNS server is operating correctly.

The bind package have been upgraded to upstream version 9.7.3., which provides a number of bug fixes and enhancements over the previous version. For more information, refer to the bind release notes. (BZ#653486)

Bug Fixes

BZ#623638

previously, bind on the 64-bit PowerPC architecture used emulated atomic operations rather than native instructions. In this updated package bind on the 64-bit PowerPC architecture uses the same native atomic operations as the PowerPC architecture.

BZ#677381

previously, the bind package generated the /etc/rndc.key file. However, generating this file used entropy from /dev/random. Consequently, installation of the bind package might have hung. The rndc.key is used by rndc utility for advanced administration commands and is no longer automatically generated during installation of the bind package. Users requiring the rndc utility should generate key themselves, via the "rndc-confgen -a" command.

BZ#623122

under certain circumstances, "named" was entering a deadlock. Consequently, "named" could not be stopped using the "/etc/init.d/named stop". In this updated package, the deadlock no longer occurs, resolving this issue.

BZ#623190

previously, the named_sdb PostgreSQL database backend failed to reconnect to the database when the connection failed during named_sdb startup. With this update, named writes error message to the system log and tries to reconnect during every lookup.

BZ#658045

previously, file conflicts prevented the i686 and x86_64 versions of bind-devel from being installed on the same machine. In this update, the file conflict is resolved and both the i686 and x86_64 bind-devel packages can be installed on the same system.

BZ#622785

previously, initscript killed all processes with the name "named" when stopping the named daemon. With this update, initscript kills only the selected one.

BZ#640538

the return codes of the "dig" utility are documented in the dig man page.

BZ#660676

previously the named.8 manpage mentioned the system-config-bind utility. This utility is not included with Red Hat Enterprise Linux 6. The man page is updated to remove the reference to the system-config-bind utility.

BZ#661663, BZ#672777

the "status" action of the named initscript would not complete when bind-sdb package was installed. These updated packages resolve this issue.

BZ#669163

when resolv.conf contained "search" keyword with no arguments host/nslookup/dig utilities failed to parse it correctly. In these updated packages, such lines are ignored.

BZ#672819

previously, the nsupdate man page incorrectly listed HMAC-MD5 as the only TSIG algorithm. In this updated package, the list of encryption algorithms was removed from the nsupdate man page. The the dnssec-keygen man page contains a complete list of usable encryption algorithms.

Enhancements

BZ#622764

the host utility now honors "debug", "attempts" and "timeout" options in resolv.conf.

BZ#623673

a new option, called DISABLE_ZONE_CHECKING, has been added to /etc/sysconfig/named. This option adds the possibility to bypass zone validation via the named-checkzone utility in initscript and allows to start named with misconfigured zones.

BZ#646932

with this update, size, MD5 and the modification time of /etc/sysconfig/named configuration file is no longer checked via the "rpm -V bind" command.

BZ#667375

Root zone DNSKEY is now included in the bind package, in the /etc/named.root.key file.

Users are advised to upgrade to these updated bind packages, which resolve these issues and add these enhancements.

1.14. bind-dyndb-ldap

1.14.1. RHBA-2011:0606 — bind-dyndb-ldap bug fix and enhancement update

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

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

Bug Fixes

BZ#658286

the plugin didn't load child zones correctly. The plugin has been fixed and now loads child zones well.

BZ#662930

named aborted when attempting to connect to a local LDAP server during boot. Now it does not abort but the administrator must call "rndc reload" when LDAP server starts to correctly fetch zones.

BZ#666244

the plugin flooded logs with too many messages. Now those messages are logged only when named is started with the "-d" (debug) parameter.

BZ#667704

the plugin was rebased to 0.2.0 bugfix release.

BZ#667727

queries for ANY type were not handled correctly, only SOA records were returned. The plugin was fixed and now all records are returned when asked.

BZ#667730

the plugin failed to reconnect to the LDAP server when SASL authentication was used. The plugin was fixed and reconnection now works.

BZ#667732

the plugin failed to delete nodes from the LDAP database when all resource records associated with the node were removed. Now the plugin deletes the empty nodes.

BZ#667733

the plugin did not emit enough information when it was configured to use invalid credentials. Now it emits enough details.

Enhancements

BZ#667729

It is now possible to specify allow-query and allow-transfer ACLs for zones.

BZ#667734

It is now possible to set timeout for queries to the LDAP server.

Users are advised to upgrade to this updated bind-dyndb-ldap package, which resolves these issues.

1.15. binutils

1.15.1. RHBA-2011:0614 — binutils bug fix and enhancement update

Updated binutils packages that fix bugs and add various enhancements are now available.

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

Bug Fixes

BZ#697703

fix occasional crash in linker

BZ#614443

fix strip to keep the address of an empty section consistent with its offset in the object

BZ#680143

if one of the input files is of a non-ELF format the linker may crash

Enhancements

BZ#578661

add support for ELF objects with more then 65535 program headers

BZ#663587

add support for the large code model on PowerPC

BZ#633448

add support for ELF core dump notes sections for extra s390 registers

BZ#631540

add support for the new instructions in the System

Users are advised to upgrade to these updated binutils packages, which resolve these issues.

1.15.2. RHBA-2011:1255 — binutils bug fix update

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

The binutils package is a collection of programming tools for the manipulation of object code in various object file formats.

Bug Fix

BZ#721079

Prior to this update, an input object file could have a non-empty .toc section but no references to the .toc entries because of a problem in the 64-bit PowerPC linker TOC editing code. As a result, various utilities of the binutils package terminated unexpectedly with a segmentation fault under certain conditions. This update handles local symbols in .toc sections correctly. Now, no more crashes occur.

Users of binutils are advised to upgrade to this updated package, which fixes this bug.

1.16. blktrace

1.16.1. RHBA-2011:0718 — blktrace bug fix update

Updated blktrace packages that fix numerous bugs are now available for Red Hat Enterprise Linux 6.

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

- blktrace (to extract event traces from the kernel)
- blkparse (to produce formatted output of event streams)
- blkiomon (for i/o monitoring - periodically generating per-device request size and request latency statistics, and providing histograms)
- btreplay (for recreating IO loads recorded by blktrace)
- btt (to analyse block i/o traces produces by blktrace)

Bug Fixes

BZ#583615

When the device list contained the same device as supplied on the command line, blktrace stopped immediately and further I/O tracing was impossible. This occurred when an error returned in BLKTRACESETUP ioctl caused the program to terminate whenever a device was duplicated in the devpaths. This patch ensures devices are not duplicated in the devpaths pool, thus fixing the problem.

BZ#619201

When blktrace was run without parameters, it incorrectly included the version number in its usage message. This resulted in the false assumption that the version number was a required parameter. This update edits the usage message so that the version number is not printed when running blktrace, blkparce or btt without parameters, avoiding any confusion.

BZ#650229

Previously, btreplay would give a 'No such file or directory' error when attempting to execute with /dev/cciss/foo because of the long path name. This was caused by missing the back conversion of underscores to slashes. This update converts the underscores to slashes to restore the device names with longer paths.

BZ#583624

Running 'blktrace -d <device> -k' once did not kill a running background trace. Running it a second time resulted in a 'BLKTRACETEARDOWN: Invalid argument' message, after which any further attempt to run it returned 'BLKTRACESETUP: No such file or directory'. This was caused by the option -k clobbering information about running a trace by the kernel (that is, blk_trace_remove), while files opened in debugfs by blktrace running in the background were not released. In this patch, the documentation is updated to remove the faulty 'kill' option. It advices to send a SIGINT signal via kill(1) to the running background blktrace for its correct termination.

BZ#650243

The documentation falsely gave the impression that blkiomon was not giving the correct output when working with a logical volume device. When working on a logical volume device, blkiomon does not understand the output of blktrace,as a logical volume device is quiet. While working with a physical device, it prints I/O statistics as expected. This patch updates the documentation to reflect this.

BZ#583695

When blkparse was run with a non-existent file as an argument, it returned no errors and the exit-code was zero. This update provides a warning message when a non-existent file is used as an argument and exits with a non-zero status.

BZ#595356

Previously, blktrace would not end after 30 seconds. Instead it would remain running until the user killed it, after which any further attempts to run it failed with an error. This was because when open_ios() failed, tracer_wait_unblock() in thread_main() waits for an event that will never occur. Because the event never occurs, any future attempts to run blktrace failed with an error. This update makes sure that unblock_tracers() is also called when an unsuccessful event occurs, (that is, when nthreads_running != ncpus).

BZ#595413

There was a mistake in the man page for btrecord. It incorrectly documented the option --input-base, which is unsupported, and the supported --max-bunch-time was undocumented. This update replaces --input-base with --input-directory, and adds the option --max-bunch to the btrecord man page.

BZ#595419

The blkiomon man page was missing elements. The options -d and --dump-lldd were not recorded. This patch adds these and a drv_data mast description to the blktrace man page.

BZ#595615

The blkparce man page was missing six elements. These were -A, --set-mask, -a, --act-mask, -D, and --input-directory. These options are now added to the blkparce man page.

BZ#595620

The blktrace man page was missing sixteen elements. These were:

- -d <dev> | --dev=<dev>
- -r <debugfs path> | --relay=<debugfs path>
- -o <file> | --output=<file>
- -D <dir> | --output-dir=<dir>
- -w <time> | --stopwatch=<time>
- -a <action field> | --act-mask=<action field>
- -A <action mask> | --set-mask=<action mask>
- -b <size> | --buffer-size
- -n <number> | --num-sub-buffers=<number>
- -l | --listen
- -h <hostname> | --host=<hostname>
- -p <port number> | --port=<port number>
- -s | --no-sendfile

- -I <devs file> | --input-devs=<devs file>
- -v <version> | --versio
- -V <version> | --version

These options are now added to the blktrace man page.

BZ#595623

The btreplay man page was missing three elements. These were -t, -x, and --acc-factor. These options are now added to the btreplay man page.

BZ#595628

The btt man page was missing four elements. These were -X, -m, --easy-parse-avgs, and --seeks-per-second. These options are now added to the btt man page.

All users of blktrace are advised to upgrade to these updated packages, which resolve these issues.

1.17. boost

1.17.1. RHBA-2011:1158 — boost bug fix update

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

Boost provides free peer-reviewed portable C++ source libraries, with emphasis on libraries which work well with the C++ Standard Library.

Bug Fix

BZ#723503

Prior to this update, the cyclic redundancy check (CRC) was not correctly computed on 64-bit architectures during decompression of gzip archives. In this update, constant-width integer types are used to compute CRC to make the results stable across all architectures.

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

1.18. btrfs-progs

1.18.1. RHEA-2011:0567 — btrfs-progs enhancement update

An updated btrfs-progs package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The btrfs-progs package provides user-space programs to create, check, modify, and correct any inconsistencies in a Btrfs file system.

Enhancement

BZ#645741

The btrfs-progs package has been updated to the latest upstream version, and newly includes the btrfs utility for easier administration of Btrfs file systems.

All users of Btrfs are advised to upgrade to this updated package, which adds this enhancement.

1.19. busybox

1.19.1. RHBA-2011:0559 — busybox bug fix update

Updated busybox packages that fixes several bugs are now available for Red Hat Enterprise Linux 6.

Busybox is a single binary containing a large number of system commands, including a shell. This package can be useful for recovering from certain types of system failures, particularly those involving broken shared libraries.

Bug Fixes

BZ#615391

Previously, the cpio applet included with busybox printed summary messages to stdout instead of stderr as the stand alone cpio does. Consequently nothing was returned to the shell when the busybox cpio applet ran. The updated applet include a patch that corrects this: the busybox cpio applet now prints summary messages to stderr, returning information to the shell as the standalone utility does.

BZ#621853

As initially released, the "busybox hwclock" utility included with Red Hat Enterprise Linux 6 honored the current Filesystem Hierarchy Standard (FHS 2.3) and assumed the adjtime state file was at /var/lib/hwclock/adjtime. If kexec was invoked to load a second kernel over a crashed kernel, this caused "busybox hwclock" to return incorrect and inconsistent values when compared with the same command running in the first kernel prior to the crash. With this update, the config file for busybox hwclock was reverted to its old behavior. It now assumes the adjtime state file is at /etc/adjtime, as was the case in FHS 2.1, and "busybox hwclock" behaves as expected when run in an initial or reloaded kernel.

BZ#633961

The "busybox awk" utility incorrectly treated all strings of digits with leading zeros as octal integer constants. This meant strings such as "0xffff" and "07777" were handled correctly but strings such as "0.531" were not. As a consequence, awk operations that correctly manipulated such strings as numbers were not handled correctly by busybox awk. With this update, the awk utility included with busybox correctly differentiates between hexadecimal and floating decimal strings and handles manipulations of the latter as expected.

All busybox users should install this update, which fixes these bugs.

1.20. ca-certificates

1.20.1. RHSA-2011:1248 — Important: ca-certificates security update

An updated ca-certificates package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact.

This package contains the set of CA certificates chosen by the Mozilla Foundation for use with the Internet Public Key Infrastructure (PKI).

It was found that a Certificate Authority (CA) issued fraudulent HTTPS certificates. This update removes that CA's root certificate from the ca-certificates package, rendering any HTTPS certificates signed by that CA as untrusted. (BZ#734381)

All users should upgrade to this updated package. After installing the update, all applications using the ca-certificates package must be restarted for the changes to take effect.

1.21. certmonger

1.21.1. RHBA-2011:0570 — certmonger bug fix and enhancement update

An enhanced certmonger package that fixes various bugs and provides several enhancements is now available for Red Hat Enterprise Linux 6.

The **certmonger** utility monitors certificate expiration and can refresh certificates with the CAs (Certifying Authorities) in networks that use public-key infrastructure (PKI).

The certmonger package has been upgraded to upstream version 0.34, which provides a number of bug fixes and enhancements over the previous version. (BZ#643561)

Bug Fixes

BZ#624142

If the **certmonger** service failed to contact a CA, the subprocess that submitted the request became defunct. This occurred because the parent process did not read the subprocess status. With this update, the parent process reads the subprocess status and there is no defunct process after a CA contact failure.

BZ#636894

Previously, after installing the certmonger utility, the certmonger service failed to start. This occurred because the package installation did not signal the system bus daemon that it needed to re-read its configuration as to allow the certmonger daemon to connect to the bus. This update fixes the bug and the certmonger service can be started right after the installation.

BZ#652047

Previously, the certmonger utility did not display a user-friendly error message when the user ran the **ipa-getcert** command with privileges that were insufficient for the system bus to allow it to communicate with the certmonger service. With this update, certmonger suppresses the original error message if a user-friendly message is available. The user can display both messages with the **-v** option.

BZ#652049

Prior to this update, the **ipa-getcert list** command did not return any output if certmonger was not tracking any certificates. With this update, the command returns a message that the certificate list is empty.

BZ#687899

Due to inappropriate SELinux policy settings, the **certmonger** daemon could not execute some of its helper processes. The updated policy now allows certmonger to run these processes and the certmonger libraries create temporary files in a location that certmonger can access.

BZ#688229

The certmonger service accepted a non-existent PIN (Personal Identification Number) file for the NSS (Network Security Services) database if the user ran the **ipa-getcert request** command with the **-p** option. This occurred because certmonger failed to detect reading errors in the file with the PIN and proceeded with an empty PIN value. With this update, such reading errors are logged and certmonger proceeded as if it had read an empty PIN value.

BZ#689776

Previously, the certmonger service terminated unexpectedly if the user attempted to use a certificate database stored in a non-existent directory. While preparing an error message to return to its client, the daemon attempted to use already-freed memory, which could have caused a segmentation fault. With this update, certmonger displays a message that the directory does not exist and remains stable in these circumstances.

BZ#690886

After installation of the ipa-client package, the ipa-client-install script runs the **ipa-getcert** command. As a consequence, the **certmonger** daemon runs its ipa-submit helper. The helper contacts the IPA server. Previously, if it received a fault message response from the server, it terminated with a segmentation fault and created a core dump; the installation failed. This happened because it attempted to dereference an uninitialized pointer while processing the fault message. With this update, the helper handles the fault message correctly and the enrollment process completes successfully.

BZ#691351

Previously, running the **getcert** command with an invalid Extended Key Usage parameter caused a segmentation fault. This happened because the command attempted to dereference a NULL pointer while attempting to report that the parameter value was not a valid OID (Object Identifier). With this update, certmonger reports that the OID validation failed and prints a message that the provided Extended Key Usage is invalid.

BZ#695672

Prior to this update, certmonger could have seemingly ignored the attempts to resubmit a certificate with changed Subject and Principal names. This occurred because the certificate changes were not saved if a certificate with the same nickname already existed in the certificate database. With this update, the certmonger utility removes the certificates with the respective nickname before storing the new certificate and the **resubmit** command works as expected.

BZ#695675

Previously, the certmonger service could have failed to resubmit certificates. This happened if the SELinux policy did not allow certmonger to write to the defined location for storing keys. With this update, the service reads information about the keys to verify that the keys had been generated and stored properly. If the reading fails, the keys are generated again.

BZ#696185

Previously, the **getcert** tool terminated unexpectedly with a segmentation fault if the user issued the **getcert start-tracking** command with changed values of the parameters Extended Key Usage, DNS, Email and Principal name. The command caused a buffer overflow in the **getcert** tool because the internal buffer in the **getcert** command was too small to hold four new values. This update enlarges the internal buffer of the command and the bug no longer occurs.

Enhancements

BZ#624143

The **ipa-getcert** and **getcert** commands did not accept the location of a passphrase, which could provide the encrypted keying material and allow monitoring of an already-issued certificate or key pair. This update adds the **-p** and **-P** options to the **getcert start-tracking** command, which allows the user to pass the utility a PIN either in a file or directly.

BZ#683926

Previously, the certmonger service did not support a verbose mode for the **ipa-getcert** command. This update adds the **--verbose** option to the command.

All users of certmonger are advised to upgrade to this updated package, which resolves these issues and provides these enhancements.

1.21.2. RHBA-2011:1280 — certmonger bug fix update

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

The certmonger service monitors certificates, warning of their impending expiration, and optionally attempting to re-enroll with supported CAs (Certificate Authorities).

Bug Fix

BZ#729803

When submitting a signing request to a Red Hat IPA (Identity, Policy, Audit) CA, certmonger is expected to authenticate using the client's host credentials, and to delegate the client's credentials to the server. Recent updates to libraries on which certmonger depends changed delegation of client credentials from a mandatory operation to an optional operation that is no longer enabled by default, which effectively broke certmonger's support for IPA CAs. This update gives certmonger the ability to explicitly request credential delegation when used with newer versions of these libraries, which introduce an API that allows certmonger to explicitly request that credential delegation be performed.

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

1.22. chkconfig

1.22.1. RHBA-2012:0416 — 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#797844

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#797843

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.

1.23. cifs-utils

1.23.1. RHBA-2011:0569 — cifs-utils bug fix update

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

The SMB/CIFS protocol is a standard file sharing protocol widely deployed on Microsoft Windows machines. This package contains tools for mounting shares on Linux using the SMB/CIFS protocol. The tools in this package work in conjunction with support in the kernel to allow one to mount a SMB/CIFS share onto a client and use it as if it were a standard Linux file system.

The cifs-utils package has been upgraded to upstream version 4.8.1, which provides a number of bug fixes over the previous version. (BZ#658981)

Bug Fixes

BZ#645127

While trying to mount a share (DFS or 'classic') with Kerberos, a "mount error(5): Input/output error" occurred due to a problem with the MIT krb5 libraries. cifs.upcall now sets the GSSAPI checksum properly in SPNEGO blobs. This is necessary for proper interoperability with EMC servers when using krb5 authentication, and allows for a successful mount .

BZ#667382

When mounting a share as root with kerberos, cifs.upcall used the ticket of root (/tmp/krb5cc_0) instead the one of the user specified with 'uid=' or 'user='. This was due to the --legacy-uid command line option for cifs.upcall not properly implementing. This patch ensures that it properly implements, allowing successful mounting of a share as root with kerberos.

BZ#669377

When two CIFS shares were mounted on the same server, each for a different user who had valid krb5 credentials, only the one mounted first could access the data. This was because cifs had a built in design limitation of a single set of credentials per mount. That limitation caused the implementation of a number of hacks to deal with it. With this patch mount.cifs now supports the 'cruid=' mount option, fixing this issue.

BZ#696951

mount.cifs did not handle numeric uid=, gid=, or cuid= options correctly, and would often return an error when they were specified. With this patch, a check is run to see if any error occurred by setting errno to 0 before the conversion. If one did then it will attempt to treat the value as a name, allowing them to be correctly handled.

All users who are using the cifs file system should update to this new package in order to take advantage of these bug fixes.

1.24. cluster and gfs2-utils

1.24.1. RHBA-2012:1189 — cluster and gfs2-utils bug fix update

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

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

Bug Fix

BZ#849047

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

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

1.24.2. RHBA-2011:0537 — cluster and gfs2-utils bug fix update

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

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

Bug Fixes

BZ#688201

cman quorum timeout is too short

BZ#595725

CMAN init script race condition has been fixed

BZ#617306

plock owner synchronization has been fixed

BZ#623810

plocks are now ignored until they written to their checkpoint

BZ#623816

plock signatures are now re-sent after a new totem ring forms

BZ#624844

post_join_delay now works after a loss and subsequent regain of quorum

BZ#634718

"service cman stop remove" now functions correctly

BZ#639018

Active cluster nodes with higher configuration version numbers are no longer killed when they join the cluster

BZ#577874

The ccs_tool man page no longer shows 'update' and 'upgrade' subcommands

BZ#614885

ccs_tool cluster configuration editing has been dropped

BZ#617234

The interaction between corosync and cman restarting independently of one another has been improved

BZ#617247

reporting of corosync's exit code has been improved

BZ#619874

cman_tool manual page no longer talks about "config version" as an argument to -r

BZ#620679

Qdiskd now stops voting and exits if removed from the configuration

BZ#624822

gfs_controld: fix plock owner in unmount

BZ#635413

Qdiskd now reports to users when the quorumd "label" attribute overrides the "device" attribute

BZ#636243

Qdiskd now has a hard limit on heuristic timeouts

BZ#649021

Pacemaker-specific versions of dlm_controld and gfs_controld have been removed since they are no longer required

BZ#657041

cman now allows users to select udpu (UDP unicast) corosync transport mechanism

BZ#663433

Qdiskd now assumes votes for each cluster node are 1 when not specified in cluster.conf

BZ#669340

The cman init script can no longer include an incorrect sysconf file

BZ#645830, BZ#618705, BZ#684020, BZ#629017, BZ#680172

The cluster.rng schema has been updated

BZ#680155

A memory leak in the XML parser has been fixed

BZ#688154

Heuristic checks are unreliable

BZ#688734

gfs2_convert no longer exits success without doing anything

BZ#628013

fsck.gfs2 was truncating directories with more than 100,000 entries

BZ#621313

fsck.gfs2 was processing some files twice

BZ#622576

fsck.gfs2 no longer crashes if journals are missing

BZ#632595

When mounting a gfs2 file system, the same device requested on the command line now appears in /proc/mounts and /etc/mtab

BZ#637913

gfs2_convert now resumes after an interrupted conversion

BZ#576640

fsck.gfs2 can now repair rgrps resulting from gfs_grow->gfs2_convert

BZ#624535

mkfs.gfs2 no longer segfaults with 18.55TB and -b512

BZ#656956

mkfs.gfs2 now supports discard request generation

BZ#663037

fsck.gfs2: reports master/root inodes as unused and fixes the bitmap

BZ#630005

gfs2_convert no longer corrupts the file system if the di_height is too large.

Enhancements

BZ#592964

Fenced now sends notifications over DBus

BZ#634623

gfs2_edit now outputs hexadecimal values in lower-case

BZ#634623

gfs2_edit now prints continuation blocks

BZ#634623

gfs2_edit's savemeta and restoremeta functions now report progress

BZ#674843

gfs2_edit has improved handling of corrupt file systems and enhanced

BZ#563901

It is now possible to prevent the cluster software from starting at boot using the kernel command line

BZ#560700

It is now possible to prevent the cluster software from starting at boot using the kernel command line

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

1.24.3. RHBA-2011:1236 — cluster and gfs2-utils bug fix update

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

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

Bug Fix

BZ#728247

Prior to this update, the "suborg" option was not allowed by the cluster configuration schema defined in the /usr/share/cluster/cluster.rng file. As a consequence, when the "suborg" option was specified for the fence_cisco_ucs agent, the cluster refused to validate the configuration schema. The "suborg" option is now properly recognized, which fixes the problem.

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

1.24.4. RHBA-2011:0958 — cluster and gfs2-utils bug fix update

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

The Red Hat Cluster Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure. Using redundant hardware,

shared disk storage, power management, and robust cluster communication and application failover mechanisms, a cluster can meet the needs of the enterprise market.

Bug Fix

BZ#720100

Previously, when a custom multicast address was configured, the configuration parser incorrectly set the default value of the time-to-live (TTL) variable for multicast packet to 0. Consequently, cluster nodes could not communicate with each other. With this update, the default TTL value is set to 1, thus fixing this bug.

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

1.25. compat-dapl

1.25.1. RHBA-2011:0696 — 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. compat-dapl contains the libraries that implement version 1.2 of the DAT API. compat-dapl is provided solely for backward compatibility.

Bug Fix

635155

Fixes an issue in which, under certain error conditions, dapl could fail to properly clean up its internal state, potentially resulting in subsequent incorrect operation.

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

1.26. coolkey

1.26.1. RHBA-2011:0765 — coolkey bug fix update

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

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

Bug Fix

BZ#210200

Previous versions of coolkey would fail to operate correctly if the pcscd daemon in the pcsc-lite package was restarted. Proper operation could be restored by restarting the application which was using coolkey, for example, the Gnome screensaver or the Gnome login screen when used with a smart card login. With this update, applications no longer need to be restarted to function properly when the pcscd daemon is restarted.

All users of coolkey are advised to upgrade to this updated package, which resolves this issue.

1.27. coreutils

1.27.1. RHBA-2011:0646 — coreutils bug fix update

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

The coreutils package contains the core GNU utilities. It is the combination of the old GNU fileutils, sh-utils, and textutils packages.

Bug Fixes

BZ#630017

The su utility was previously not built with PIE and RELRO enabled, as they were in Red Hat Enterprise Linux 5. In this update, it is built as a PIE executable and is using RELRO protection.

BZ#628212

Previously, when reading a line longer than 16KiB, the tac utility reallocated its primary buffer. Before exiting, the tac utility tried to free the already freed original buffer, which caused a utility crash after a double free error displayed. This was fixed and the tac utility no longer frees an already freed buffer.

BZ#598631

Previously, the hardware control flow, DTRDSR, was implemented via TC{SG}ETX. This was changed to TC{SG}ET ioctl, which caused the CDTRDSR support in stty to fail. This was fixed to allow stty to correctly handle CDTRDSR control flow.

BZ#683799

Previously, the internalization patch for coreutils had an unsafe initialization of char* bufops that left bufops uninitialized or initialized to NULL on the first usage. This behavior called memmove from an incorrect address, namely from address 0 and size 0. This is now fixed and bufops is correctly initialized for the first use.

BZ#649224

Previously, when the multibyte LC_TIME differed from LC_CTYPE, an assertion failure caused the sort utility to crash irrespective of the parameters provided to it. This is fixed to prevent a crash when the sort utility is run and now works as expected.

BZ#660033

Previously, the information page about 8-bit octal values did not mention checking if the value was lower than 256. Due to this, when a command like "/bin/echo -e '\0610'" was used, the results were not accurate. This is now fixed to provide more accurate information about the behavior of octal values.

BZ#614605

Previously, when the dd utility used pipes, it read and wrote partial blocks. When the size of the block written was shorter than the specified maximum output block size, the "oflag=direct" would turn off, which resulted in degraded I/O performance. The workaround for this behavior, which involves the addition of "iflag=fullblock" is now available in the information documentation.

BZ#662900

Previously, documentation for tail command's --sleep-interval option did not outline the results of inotify support. This is now fixed and the documentation states that with inotify support, the --sleep-interval option is only relevant when the tail command reverts to the old polling-based method.

BZ#609262

Previously, the coreutils information page was not sufficiently clear about behavior when multiple parent and leaf node directories are created. This is now fixed to incorporate additional information in the coreutils information page about the @option mode and its behavior when combined with the --parents option.

All coreutils users are advised to upgrade to these updated packages, which resolve these issues.

1.28. corosync

1.28.1. RHBA-2012:1215 — 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#849552

Previously, the corosync-notifyd daemon, with dbus output enabled, waited 0.5 seconds each time a message was sent through dbus. Consequently, corosync-notifyd was extremely slow in producing output and memory of the Corosync server grew. In addition, when corosync-notifyd was killed, its memory was not freed. With this update, corosync-notifyd no longer slows down its operation with these half-second delays and Corosync now properly frees memory when an IPC client exits.

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

1.28.2. RHBA-2011:0764 — corosync bug fix update

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

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

Bug Fixes

BZ#619496

Multicast emulation caused an extra delay to the multicast packet transmission, causing unnecessary retransmission of the packet. This update adds the "miss_count_const" constant allowing the user to specify how many times a message is checked before retransmission occurs.

BZ#619918

When denied permissions from SELinux, corosync failed with a segmentation fault. Corosync now passes an error back to the API user when it is unable to create a connection between the server and client instead of causing a segmentation fault.

BZ#613836

When provided an invalid multicast address, corosync failed without errors. This is now fixed, thus corosync displays an error when given an invalid multicast address.

BZ#639023

Corosync client libraries delayed for 2 seconds before they displayed an error on a shut down. This is now fixed, thus the exited flag value before and after sem_wait is checked. If the value is true, ERR_LIBRARY displays.

BZ#640311

The default TTL value in multicast was 1, preventing use on a routed network. The TTL value is now configurable in the corosync configuration file, thus multicast can now be used on a routed network.

BZ#684930, BZ#684920

BZ#640311 introduced a regression.

BZ#665165

Shared memory no longer is leaked if the corosync server unexpectedly exits while connected to corosync clients.

BZ#626962

Running multiple instances of corosync simultaneously would succeed, causing local node errors. This is now fixed to prevent initialization of multiple instances of corosync.

BZ#614104

If cman ran the corosync init script, it would cause the corosync init script to be blocked. This is now fixed to allow corosync to create a Pid file and to allow cman to run corosync.

BZ#629380

Corosync was unable to capture system events and notify the user about them. With this fix, SNMP MIB and daemon are added for system event notification via DBUS and SNMP.

BZ#675859

Member objects in corosync were not found due to validation failure. This is fixed with an addition to the objdb file, thus validation for SNMP/DBUS integration is now successful.

BZ#675741

The corosync build contained invalid version information, which caused rpmdiff to warn the user about version information changes. This was fixed, thus pkgconfig files are now correctly configured to display version as 1.2.3.

BZ#680258

Corosync rebuilds succeeded only on fresh installations due to a regression issue. This is now fixed, thus corosync now rebuilds on existing installations as well.

BZ#675099

A ring id file smaller than 8 bytes caused corosync to abort. This was fixed by recreating the ring id file, thus corosync now does not abort due to the ring id file.

BZ#677975

Inconsistent cluster.conf files amongst nodes caused a memory leak. This is now fixed, thus a configuration reload via cman_tool no longer causes a memory leak.

BZ#675783

During the recovery phase, aisexec exited unexpectedly, resulting in a lost network token. This is now fixed, thus aisexec no longer exits due to a lost token.

BZ#568164

UDPU transport is added, which simulates multicast via UDP unicast. This adds a third transport option to broadcast and multicast in a cluster.

BZ#688691

Fix abort that happens in rare circumstances during shutdown.

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

1.28.3. RHBA-2012:0736 — 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#828431

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.

1.28.4. RHBA-2012:0535 — 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#810916

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.

1.28.5. RHBA-2012:0375 — 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#791235

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.

1.28.6. RHBA-2011:1361 — corosync bug fix update

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

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

Bug Fixes

BZ#726608

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#727962

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#734997

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.

1.29. cracklib

1.29.1. RHBA-2011:0202 — cracklib bug fix update

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

CrackLib is a password-checking library that is used to help enforce password quality controls.

Bug Fixes

BZ#583932

Manual pages for the cracklib-check, cracklib-format, and create-cracklib-dict utilities have been added.

BZ#627449

The Simplified Chinese (zh_CN) translation of one of the error messages the library can produce has been corrected, and no longer contains untranslated strings.

All users of cracklib are advised to upgrade to these updated packages, which resolve these issues.

1.30. crash

1.30.1. RHBA-2011:0561 — crash bug fix and enhancement update

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

The crash package provides a self-contained tool that can be used to investigate live systems, and kernel core dumps created from the netdump, diskdump, kdump, and Xen/KVM "virsh dump" facilities from Red Hat Enterprise Linux.

The crash package has been upgraded to upstream version 5.1.1, which provides a number of bug fixes over the previous version. (BZ#649070)

Bug Fixes

BZ#637735

On 64-bit x86 architectures, using the "bt" command to analyze core dumps from kernel 2.6.27 or later caused it to display an invalid "vgettimeofday" frame above the topmost "system_call_fastpath" frame, followed by two read error messages similar to the following:

```
bt: read error: kernel virtual address: ffffffffff600000  type:
"gdb_readmem_callback"
```

This error no longer occurs, and the "bt" command now produces correct results for these kernels.

BZ#649050

When analyzing a KVM dump file from a 64-bit x86 guest system, the crash utility failed to determine the starting RIP and RSP hooks. This rendered it unable to produce a correct backtrace for tasks that were either running in user space when the "virsh dump" operation was performed on a live guest, or that were running on interrupt or exception stacks. With this update, the RIP and RSP hooks for a

particular dump file are now determined by using the content of the per-CPU registers in the CPU device format. As a result, the "bt" command no longer produces incorrect backtraces for such dump files.

BZ#649051

When analyzing a KVM dump file from an x86 guest system, the crash utility was unable to determine the starting EIP and ESP hooks, and produced an invalid backtrace. With this update, the crash utility has been updated to use the 64-bit CPU device format in x86 KVM dump files by default, and only use the 32-bit format when it is determined that the host machine was running a 32-bit kernel. As a result, running the "bt" command when analyzing such a dump file now produces a correct backtrace.

BZ#649053

When creating a KVM dump file, the "virsh dump" operation marks all non-crashing CPUs as offline. Due to an incorrect use of the "cpu_online_map" mask to determine the CPU count, previous version of the crash utility may have reported a wrong number of CPUs when analyzing dumps created by the "virsh dump" command on x86 guest systems. With this update, the underlying source code has been adapted to use the "cpu_present_map" mask instead, so that the crash utility reports the correct number of CPUs.

BZ#682129

Prior to this update, an attempt to display a backtrace of a non-active swapper task on a 32-bit x86 architecture could cause the crash utility to display the following message:

```
bt: cannot resolve stack trace:
#0 [c09f1ef4] ia32_sysenter_target at c08208ce
```

This update applies a patch that resolves this issue, and the crash utility now resolves such backtraces as expected. Additionally, this update ensures that the crash utility is no longer negatively affected by the changes that were introduced in kernel 2.6.32-112.

Enhancements

BZ#633449

The crash utility has been updated to provide support for dump files created on the IBM System z architecture.

BZ#637197

The crash utility now supports compressed and/or filtered dump files generated by the makedumpfile utility on IBM System z.

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

1.31. crda

1.31.1. RHEA-2011:0550 — crda enhancement update

An updated crda package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The crda package contains the Central Regulatory Domain Agent, which provides the kernel with the wireless regulatory rules for a given jurisdiction.

Enhancement

654066

This updated crda package enhances the kernel with the most current information with regard to wireless regulatory rules, and ensures that these updated rules are enforced.

All users are advised to upgrade to this updated package, which adds this enhancement.

1.32. cronie

1.32.1. RHBA-2011:0788 — cronie bug fix update

Updated cronie packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

Cronie contains the standard UNIX daemon crond that runs specified programs at scheduled times and related tools. It is a fork of the original vixie-cron and has security and configuration enhancements like the ability to use pam and SELinux.

Bug Fixes

BZ#615107

The initscript output written to /var/log/boot.log contained a double output of "OK", printed by /etc/init.d/crond and daemon. This error has been corrected: the echo from /etc/init.d/crond is removed, thus the output is now as expected.

BZ#624043

Cronie didn't close file descriptor, which caused other applications such as anacron that are subsequently started by cronie to inherit the file descriptor. This caused SELinux to prevent /bin/bash access. With this update, the file descriptor is no longer inherited by other applications, thus SELinux no longer prevents /bin/bash access.

BZ#675077

An incorrect option in the bash script caused anacron to run daily instead of hourly if the /var/spool/anacron/cron.daily file existed. The error has been corrected: the bash script option is fixed and anacron now runs once a day if the /var/spool/anacron/cron.daily file exists.

BZ#676040

RELRO flags were previously not set by default from crond. This is now fixed so that cronie is compiled with RELRO protection enabled.

BZ#676081

The /usr/bin/crontab was set to use both setuid and setgid permissions, but this was changed to use only setuid.

BZ#677364

Multiple code quality improvements were made, which include: - In src/crontab.c, mkstemp expects six X's to be replaced with digits at the end of each filename. This fix removes the extra X's. - In src/security.c, ccon was not freed after a return. This is fixed and ccon is now freed using context_free. - In anacron/run_job.c, fdin was tested before being initialized. This is fixed to ensure that fdin is now initialized prior to testing.

All users of cronie are advised to upgrade to this updated package, which resolves these issues.

1.33. cryptsetup-luks

1.33.1. RHBA-2011:0597 — cryptsetup-luks bug fix and enhancement update

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

The cryptsetup-luks packages provide the utility allowing users to set up encrypted devices with the Device Mapper and the dm-crypt target.

The cryptsetup-luks package has been upgraded to upstream version 1.2.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#658817)

In addition, these updated cryptsetup-luks packages provide fixes for the following bugs:

BZ#612963

Previously, cryptsetup printed twice the error message notifying the user that the queried device did not exist. With this update, the underlying code was changed and the error message is displayed once.

BZ#623121

Prior to this update, when the user attempted to encrypt a device with the MD4 or MD5 hash algorithm, cryptsetup did not alert the user that the encryption with those algorithms was not supported, had failed, and that therefore the device could not be used. With this update, cryptsetup terminates the process and prints a message advising the user to check if the required encryption method is supported.

BZ#674825

Previously, cryptsetup did not remove keys as soon as possible from device control buffers and therefore did not follow FIPS (Federal Information Processing Standard). With this update, the underlying code has been changed and the keys are removed from the buffers as soon as possible.

BZ#677634

Previously, if the user issued the "cryptsetup luksRemoveKey" command with the "--key-file" parameter, the command removed the key defined in the standard input. With this update, such command removes the key defined in the "--key-file" parameter.

BZ#692512

Prior to this update, when updating with the "yum update" command, the device-mapper-libs package was not updated. This occurred because the previous version of the cryptsetup package was compatible with any version of the package. This update adds the dependency to the cryptsetup package and the device-mapper-libs is updated to provide the compatible device-mapper-libs package.

BZ#693371

Previously, when running in FIPS mode, the salt for PBKDF2 (Password-Based Key Derivation Function) was generated with the /dev/urandom device. According to NIST Special Publication 800-132, all or a portion of the salt must be generated with an approved random number generator. With this update, the salt is generated with the FIPS RNG (Random Number Generator) and the criterion is met.

Enhancements

BZ#663869

With this update, cryptsetup uses a FIPS certified random number generator for generation of volume keys when running in FIPS mode.

BZ#663870

This update adds the integrity check of the cryptsetup binary and library for FIPS mode.

Users are advised to upgrade to these updated cryptsetup-luks packages, which resolve these bugs and add these enhancements.

1.33.2. RHBA-2011:0884 — cryptsetup-luks bug fix update

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

The cryptsetup-luks packages provide a utility which allows users to set up encrypted devices with the Device Mapper and the dm-crypt target.

Bug Fixes

BZ#713456

When the cryptsetup or libcryptsetup utility was run in FIPS (Federal Information Processing Standards) mode, the "Running in FIPS mode." message was displayed during initialization of all commands. This sometimes caused minor issues with associated scripts. This bug has been fixed and the message is now displayed only in verbose mode.

BZ#709055

Previously, the libcryptsetup crypt_get_volume_key() function allowed to perform an action not compliant with FIPS. To conform FIPS requirements, the function is now disabled in FIPS mode and returns an EACCES error code to indicate it.

Note that the "luksDump --dump-master-key" command and the key escrow functionality of the volume_key package are also disabled in FIPS mode as a consequence of this update.

Users of cryptsetup-luks are advised to upgrade to these updated packages, which fix these bugs.

1.34. cups

1.34.1. RHBA-2011:0715 — cups bug fix update

Updated cups packages resolving several issues are now available for Red Hat Enterprise Linux 6.

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

Bug Fixes

BZ#580604

Some printers were incorrectly reporting ink and toner levels via SNMP backend. Support for an SNMP quirk has been added and enabled via the PPD file.

BZ#614908

Previously, lpstat -p always reported job id as '-0'. This was because the jobstate was never IPP_JOB_PROCESSING due to an SVN revision upstream. This patch fixes this issue by adding the attributes needed for jobs.

BZ#616864

The previous 8MB default RIP cache size was insufficient for modern high-resolution (color/photo) printing. This was because filters such as pstoraster could fail. This update increases the default RIP cache size to 128MB to fix this issue.

BZ#624441

If the cupsd daemon was stopped while a job was being sent to a printer using a given backend, that backend was restarted multiple times before the CUPS scheduler actually terminated. In this updated package, the CUPS scheduler tracks whether it is shutting down and does not automatically start new jobs if so.

BZ#632180

The 'restartlog' action was missing in Initscript usage output, preventing its usage. This update adds it.

BZ#634931

Several rpmlint errors and warnings were fixed: - fixing the character encoding in CREDITS.txt - marking the D-Bus configuration file as config file - not marking MIME types and convs files as config files (overrides can be placed as new *.types/*.convs files in /etc/cups) - not marking banners as config files, instead new banners are provided - not marking initscript as a config file - not marking templates and www files as config files, instead a different ServerRoot setting is used to provide local overrides. Please note that a recent security fix required a change to template files - providing a versioned LPRng symbol for rpmlint - using mode 0755 for binaries and libraries where appropriate - moving /etc/cups/pstoraster.convs to /usr/share/cups/mime/ - moving the cups-config man page to the devel sub-package

BZ#642448

Red Hat Enterprise Linux 4 CUPS clients use the character set specified in LANG as the charset attribute in CUPS IPP requests, where Red Hat Enterprise Linux 5 and 6 ignore this, leading to incompatibilities. In these updated packages the CUPS server has been adjusted so that non-UTF-8 clients (e.g. Red Hat Enterprise Linux 4 clients) continue to be accepted.

BZ#646814

The subpackage cups-php consumed library libcups.so2 from subpackage cups-libs even though it did not have an explicit package version requirement. In this update cups-php subpackage now explicitly requires cups-libs of the same version and release.

BZ#654667

The ipp, socket and lpd backends were treating name resolution failures as a permanent error. Because these types of failures can be temporary, the tolerance for DNS failures has been added.

BZ#659692

Previously, the CUPS service did not stop normally if it was running when halting the system or a reboot was performed. Instead, it had to be killed in the final stage of reboot or shut down. This update fixes Initscript so the service is correctly stopped on reboot or halt.

BZ#668010

When the cupsd daemon was running with SELinux features enabled, the file descriptor count was increasing over time until its resources ran out. With this update, the resources are allocated only once so they do not leak file descriptors.

BZ#672614

There was a small typo in sample snmp.conf file. It is fixed in this update.

All users of cups are advised to upgrade to these updated packages, which resolve these issues.

1.34.2. RHBA-2011:1316 — cups bug fix update

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

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

Bug Fix

BZ#736304

The MaxJobs directive controls the maximum number of print jobs that are kept in memory. Previously, once the number of jobs reached the limit, the CUPS system failed to automatically purge the oldest completed job from the system to make room for a new one. This bug has been fixed, and the jobs beyond the limit are now properly purged in the described scenario.

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

1.35. curl

1.35.1. RHSA-2011:0918 — Moderate: curl security update

Updated curl 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.

cURL provides the libcurl library and a command line tool for downloading files from servers using various protocols, including HTTP, FTP, and LDAP.

Security Fix

CVE-2011-2192

It was found that cURL always performed credential delegation when authenticating with GSSAPI. A rogue server could use this flaw to obtain the client's credentials and impersonate that client to other servers that are using GSSAPI.

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

1.35.2. RHBA-2011:0573 — curl bug fix update

Updated curl packages that fix bugs in HTTPS, FTP, LDAP and proxy kerberos authentication are now available for Red Hat Enterprise Linux 6.

cURL is a tool for getting files from HTTP, FTP, FILE, LDAP, LDAPS, DICT, TELNET and TFTP servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity. cURL offers many useful capabilities, like proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.

Bug Fixes

BZ#690273

libcurl introduced a segfault where a RHEL 6.1 machine registered at RHN would result in a segmentation fault (core dumped) after running "yum clean all" and "yum update" respectively. "CERT_GetDefaultCertDB" is now used to prevent a segmentation fault after the "yum clean all" and "yum update" sequence.

BZ#623663

libcurl HTTPS connections failed with a CURLE_OUT_OF_MEMORY error when given a certificate file name without a "/". This is now fixed to treat such a string as certificate nickname and if a file with the same name exists and libcurl runs in verbose mode, a warning is issued. The updated documentation now suggests to use the "./" prefix to load a file from the current directory.

BZ#669048

A rebuild operation for curl failed if the libnih-devel package was installed. This is now fixed to allow a rebuild whether libnih-devel is installed, not installed or has a broken installation.

BZ#669702

libcurl ignored the CA path provided in CURLOPT_CAPATH and consequently curl ignored the "--capath" argument provided. This is fixed so that libcurl now uses the value provided with the "--capath" argument.

BZ#670802

libcurl leaked memory and eventually resulted in a failed NSS shutdown when more than one CA certificate was loaded. This is now fixed so that libcurl works as expected when more than one CA certificates is loaded.

BZ#678594

libcurl leaked memory when an SSL connection failed. This is now fixed to prevent the memory leak during an SSL connection failure.

BZ#651592

libcurl FTP protocol implementation was unable to handle server session timeouts correctly. This is now fixed so that libcurl drops the connection when a 421 timeout response is received.

BZ#655134

libcurl failed when an LDAP request was sent using curl through a HTTP proxy in tunnel mode (curl option "-p" or "--proxytunnel"). Curl tried to connect directly to the LDAP server via the proxy port and consequently failed. This is now fixed to allow libcurl LDAP connections through HTTP proxies to work as expected.

BZ#625685

libcurl was unable to authenticate http proxies via Kerberos. This is now fixed and libcurl can successfully authenticate http proxies via Kerberos.

BZ#678580

When libcurl connected a second time to an SSL server with the same server certificate, the server's certificate was not re-authenticated because libcurl confirmed authenticity before the first connection to the server. This is fixed by disabling the SSL cache when it is not verifying a certificate to force the verification of the certificate on the second use.

BZ#684892

Kerberos authentication was broken for reused curl handles, which prevented "git clone"' from working with Kerberos authenticated web servers. This is now fixed to allow "git clone" operations to successfully authenticate and carry out operations.

BZ#694294

It was not possible to use two distinct client certificates to connect two times in a row to the same SSL server. This is now fixed to allow two different client certifications to connect to the same SSL server.

Users of curl should upgrade to these updated packages, which contain back-ported patches to correct these issues. All running applications using libcurl must be restarted for the update to take effect.

1.35.3. RHBA-2011:1186 — curl bug fix update

Updated curl packages that resolve an issue are now available Red Hat Enterprise Linux 6.

The curl packages provide the libcurl library and the cURL command line tool for transferring data using various protocols, including HTTP, FTP, FILE, LDAP, TELNET, TFTP, SCP. Both, libcurl and cURL, support many useful capabilities, such as user authentication, proxy support, FTP uploading, HTTP POST and PUT methods, SSL certificates, and file transfer resume.

Bug Fix

BZ#727884

As a solution to a security issue, GSSAPI credential delegation was disabled, which broke the functionality of the applications that were relying on delegation, which was incorrectly enabled by libcurl. To fix this issue, the CURLOPT_GSSAPI_DELEGATION libcurl option has been introduced in order to enable delegation explicitly when applications need it. All applications using GSSAPI credential delegation can now use this new libcurl option to be able to run properly.

All users of cURL and libcurl are advised to upgrade to these updated packages, which resolve this issue. All running applications using libcurl have to be restarted for the update to take an effect.

1.36. cyrus-imapd

1.36.1. RHSA-2011:0859 — Moderate: cyrus-imapd security update

Updated cyrus-imapd 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 cyrus-imapd packages contain a high-performance mail server with IMAP, POP3, NNTP, and Sieve support.

Security Fix

CVE-2011-1926

It was discovered that cyrus-imapd did not flush the received commands buffer after switching to TLS encryption for IMAP, LMTP, NNTP, and POP3 sessions. A man-in-the-middle attacker could use this flaw to inject protocol commands into a victim's TLS session initialization messages. This could lead to those commands being processed by cyrus-imapd, potentially allowing the attacker to steal the victim's mail or authentication credentials.

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

1.36.2. RHSA-2011:1317 — Important: cyrus-imapd security update

Updated cyrus-imapd 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 cyrus-imapd packages contain a high-performance mail server with IMAP, POP3, NNTP, and Sieve support.

Security Fix

CVE-2011-3208

A buffer overflow flaw was found in the cyrus-imapd NNTP server, nntpd. A remote user able to use the nntpd service could use this flaw to crash the nntpd child process or, possibly, execute arbitrary code with the privileges of the cyrus user.

Red Hat would like to thank Greg Banks for reporting this issue.

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

1.36.3. RHSA-2011:1508 — Moderate: cyrus-imapd security update

Updated cyrus-imapd packages that fix two 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The cyrus-imapd packages contain a high-performance mail server with IMAP, POP3, NNTP, and Sieve support.

Security Fixes

CVE-2011-3372

An authentication bypass flaw was found in the cyrus-imapd NNTP server, nntpd. A remote user able to use the nntpd service could use this flaw to read or post newsgroup messages on an NNTP server configured to require user authentication, without providing valid authentication credentials.

CVE-2011-3481

A NULL pointer dereference flaw was found in the cyrus-imapd IMAP server, imapd. A remote attacker could send a specially-crafted mail message to a victim that would possibly prevent them from accessing their mail normally, if they were using an IMAP client that relies on the server threading IMAP feature.

Red Hat would like to thank the Cyrus IMAP project for reporting the CVE-2011-3372 issue. Upstream acknowledges Stefan Cornelius of Secunia Research as the original reporter of CVE-2011-3372.

Users of cyrus-imapd are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the update, cyrus-imapd will be restarted automatically.

1.37. dapl

1.37.1. RHBA-2011:0695 — dapl bug fix update

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

The dapl package provides a user space implementation of the DAT 2.0 API, and is built to natively support InfiniBand/iWARP network technology.

Bug Fixes

BZ#626541

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#626541

Previously, the function dapls_evd_dto_wait() returned, under certain circumstances, an error code when a thread was waiting on the function and the thread received a signal. Due to this behavior, the application failed. With this update, the application retries the request.

BZ#636596

Previously, applications that utilize uDAPL could not use the RDMA over converged Ethernet (RoCE) feature. This update adds these additional entries to the dat.conf file.

BZ#649360

The dat_ia_open() function could, under certain circumstances, fail to return. With this update, the function returns as expected.

BZ#667742

Under certain circumstances dapl could fail to clean up its internal state, resulting in subsequent usage of the library to fail. With this update, the internal state is cleaned up as expected and the library can be used without further problems.

BZ#637980

Previously, dapl could, under certain circumstances, fail to free allocated memory, potentially causing the application to run out of memory and fail. Now, dapl frees all allocated memory.

All dapl users should upgrade to these updated packages, which fix these bugs.

1.38. dbus

1.38.1. RHSA-2011:1132 — 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.

Security Fix

CVE-2011-2200

A denial of service flaw was found in the way the D-Bus library handled endianness conversion when receiving messages. A local user could use this flaw to send a specially-crafted message to dbus-daemon or to a service using the bus, such as Avahi or NetworkManager, possibly causing the daemon to exit or the service to disconnect from the bus.

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.

1.39. device-mapper-multipath

1.39.1. RHBA-2012:1400 — device-mapper-multipath bug fix update

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

The device-mapper-multipath packages provide tools for managing multipath devices using the device-mapper multipath kernel module.

Bug Fixes

BZ#863462

When certain multipathd threads started their operation, they did not check if the multipathd daemon

was being shut down. Consequently, multipathd could terminate unexpectedly with a segmentation fault on shutdown. With this update, the multipathd threads properly quit if they detect multipathd is shutting down and the crashes no longer occur.

BZ#866553

Previously, multipathd was removing a map twice if it failed to create a multipath device when adding a path device. Consequently, multipathd accessed already freed memory and in some cases terminated unexpectedly when a new path device was added. With this update, multipathd no longer performs the second remove operation and the crashes no longer occur in the described scenario.

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

1.39.2. RHBA-2011:0725 — device-mapper-multipath bug fix and enhancement update

Updated device-mapper-multipath packages that fix several bugs and add various enhancements are now available for Red Hat Linux 6.

The device-mapper-multipath packages provide tools for multipath device management with the device-mapper multipath kernel module.

Bug Fixes

BZ#611779

If you sent the **multipathd** daemon a command consisting only of spaces, the daemon terminated unexpectedly with a segmentation fault. With this update, the daemon is able to handle such commands and no longer crashes in this circumstance.

BZ#635088

Prior to this update, the daemon occasionally grouped paths incorrectly because the multipathd daemon did not recalculate path groups when restoring paths. Now, when a new path goes online, the multipathd daemon verifies whether it needs to recalculate path groups, and refreshes and reads all priorities.

BZ#636071

Previously, if the user edited configuration information with the **mpathconf** command, the process could have failed. This happened when the user ran the command without any additional arguments due to a conflict of the environment variable **DISPLAY** with the program variable **DISPLAY**. With this update, all variables are unset when the script is started and the **DISPLAY** program variable is renamed. The environment variable **DISPLAY** remains unchanged when the **mpathconf** is issued and the command works as expected.

BZ#645605

The DM-Multipath application marked paths as failed if it was unable to determine if a path was offline. With this update, multipath calls the **path_checker** function to determine the path state in such cases and the problem no longer occurs.

BZ#650797

Previously, multipathd displayed no **tgt_node_name** value for iSCI devices. This occurred because multipath used the FC (Fibre Channel) path from the sysfs file system to obtain **tgt_node_name** for iSCI devices. With this update, multipath first tries to acquire the FC path. If it fails, it uses the iSCI

target name for the device.

BZ#651389

Previously, if you set **dev_loss_tmo** to a value greater than 600 in **multipath.conf** without setting the **fast_io_fail_tmo** value, the **multipathd** daemon failed to apply the setting. With this update, the **multipathd** daemon sets **dev_loss_tmo** for values over 600 correctly, as long as **fast_io_fail_tmo** is also set in the **/etc/multipath.conf** file.

BZ#662731

DM-Multipath could have terminated unexpectedly if the **multipath.conf** file contained parameters with no value. This occurred because it was trying to acquire the string length of an optional value before verifying that a value was actually defined. With this update, **multipathd** first checks if the value exists and the bug is fixed.

BZ#622569

On a non-disruptive upgrade (NDU), all paths to EMC Symmetrix arrays could have failed, which caused **multipathd** to fail all outstanding input/output. DM-Multipath now has a new default configuration for EMC Symmetrix arrays that queues input/output for up to 30 seconds if all paths are down and the problem no longer occurs.

BZ#623644

The **multipathd** daemon consumed excessive memory when iSCI devices were unloaded and reloaded. This occurred because the daemon was caching unnecessary **sysfs** data, which caused memory leaks. With this update, **multipathd** no longer caches these data; it frees the data when the associated device is removed.

BZ#680480

During a double path failure, the **sysfs** device file is removed and the **sysdev** path attribute is set to NULL. The **sysfs** device cache is indexed by the actual **sysfs** directory, and **/sys/block/*pathname*** is a symlink. Prior to this update, if the path was deleted, **multipathd** was not able to find the actual directory, which **/sys/block/*pathname*** pointed to, and searched the cache. With this update, **multipathd** verifies that sysdev has **NULL** value before updating it.

BZ#681144

When a path was removed, the **multipathd** daemon did not always remove the path **sysfs** device from its cache. The daemon kept searching the cache for the device and created **sysfs** devices without the vecs lock held. Because of this, paths could have pointed to invalid **sysfs** devices and caused **multipathd** to crash. The **multipathd** daemon now always removes the **sysfs** device from cache when deleting a path and accesses the cache only with the vecs lock held.

Enhancements

BZ#576919

The **log_checker_err** option was added to the **multipath.conf** defaults section. By default, the option is set to **always** and a path checker error is logged continuously. If set to **once**, **multipathd** logs a path checker error once at logging level **2**. Any later errors are logged at level **3** until the device is restored.

BZ#599690

Previously, the **defaults** section of the **multipath.conf** man page implied that the settings defined in the section became default and overrode the implied settings. Since the HWTABLE cannot be overridden, the wording of the man page has been changed.

BZ#628095

Previously, DM-Multipath did not print any messages when errors were detected in the **multipath.conf** file. With this update, multipath prints warning messages that inform the user that the configuration files contains invalid or duplicate options and the bug is fixed.

BZ#632734

This update adds the default configuration for Virtual SCSI disks.

BZ#633643

This update adds the default configuration for NEC Storage M.

BZ#636213

This update adds the default configuration for HP P2000.

BZ#636246

This update adds the default configuration for HP OPEN devices.

BZ#644111

If the **initramfs** file system was not rebuilt when a new storage device was added to the system, the new device could have been assigned a **user_friendly_names** value that matched the **user_friendly_names** value already-assigned to another device. This device then stopped working correctly. The multipathd daemon now accepts a **-B** option, which makes the **user_friendly_names** bindings file read-only. When initramfs calls multipath with the **-B** option, devices without a binding to a user_friendly_names use their World Wide Identifier (WWID).

BZ#650664

Previously, the DM-Multipath did not prompt the user to increase the maximum number of open file descriptors (max_fds) if it failed to open a file descriptor due to receiving an EMFILE error. With this update, it prints out a message advising the user to do so.

BZ#602883

Previously, the **multipathd** deamon printed **add map** messages whenever it received a change uevent. In order not to clutter logs, multipathd now only prints **add map** messages for the change uevents of the devices that are not yet monitored.

BZ#639037

Previously, DM-Multipath did not set a default value for the no_path_retry parameter for Hitachi R700 devices. With this update, the parameter value for the devices is set to **6** by default.

BZ#696157

The **multipathd** daemon could have terminated unexpectedly with a segmentation fault on a multipath device with the **path_grouping_policy** option set to the **group_by_prio** value. This occurred when a device path came online after another device path failed because the multipath daemon did not manage to remove the restored path correctly. With this update multipath removes and restores such paths correctly.

Users are advised to upgrade to these updated device-mapper-multipath packages, which resolve these issues and add these enhancements.

1.39.3. RHBA-2012:0501 — 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#802431

Device-Mapper Multipath uses certain regular expressions in the built-in device configurations to determine a multipath device so that the correct configuration can be applied to the device. Previously, some regular expressions for the device vendor and product ID were set too broad. As a consequence, some devices could be matched with incorrect device configurations. With this update, the product and vendor regular expressions have been set more strict so that all multipath devices can now be properly configured.

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

1.39.4. RHBA-2011:1287 — device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix a bug 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#732384

When deleting a multipath device while checking a path, the multipathd daemon did not abort the path check. As a consequence, the daemon terminated when trying to access multipath device information. The problem has been fixed and the multipathd daemon now aborts the path check when deleting a multipath device.

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

1.40. dhcp

1.40.1. RHSA-2011:1160 — Moderate: dhcp security update

Updated dhcp packages that fix two 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address.

Security Fixes

CVE-2011-2748, CVE-2011-2749

Two denial of service flaws were found in the way the dhcpd daemon handled certain incomplete request packets. A remote attacker could use these flaws to crash dhcpd via a specially-crafted request.

Users of DHCP should upgrade to these updated packages, which contain a backported patch to correct these issues. After installing this update, all DHCP servers will be restarted automatically.

1.40.2. RHBA-2011:0697 — dhcp bug fix and enhancement update

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

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. DHCPv6 is the DHCP protocol version for IPv6 networks.

Bug Fixes

BZ#625846

Previously, it was impossible to configure the dhcrelay service to run the dhcrelay daemon with additional arguments. With this update, a DHCRELAYARGS variable is available for the /etc/sysconfig/dhcrelay configuration file, which allows additional arguments to be passed to the dhcrelay daemon properly.

BZ#627257

Previously, the dhclient utility did not log its PID (process identifier) in syslog entries, making troubleshooting in systems with multiple running dhclients difficult. Now, the dhclient utility logs its PID properly.

BZ#631071

Previously, the dhclient utility sometimes parsed date strings in lease files incorrectly, resulting in syntax error messages in its output. This bug has been fixed and the dates in the lease files are now parsed with no error messages given.

BZ#637763

When the dhclient utility was updating a "search" entry in the /etc/resolv.conf file, it sometimes did not add a missing domain part. This was inconsistent with NetworkManager behavior. Now, while updating the "search" entry, the dhclient utility always adds the domain part of the host name given to the client if it is missing.

BZ#672551

Previously, the dhcpd service with IPv6 support sometimes created a lease file that it was unable to parse. Consequently, once the service was restarted, it went into a loop and could not start. This bug has been fixed and now the service is able to properly parse all lease files it generates.

BZ#681721

DHCP servers at some ISPs send to clients the "interface-mtu" option with the value of 576. Such a low MTU (Maximum Transmission Unit) can cause throughput problems with UDP traffic, among other things. With this update, the dhclient utility now sets the interface MTU only if the value obtained from the server is higher than 576.

BZ#613683

Previously, the dhclient package was missing its LICENSE file. With this update, the file has been added.

Enhancements

BZ#558641

The dhcp package now provides an implementation of Classless Static Route Options for DHCPv4 (RFC 3442). It can supply network route configuration to a large number of hosts without individual configuration of each one.

BZ#660681

The dhcp package now provides support for IPoIB (IP over InfiniBand) interfaces.

Users of dhcp are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.41. dmidecode

1.41.1. RHBA-2011:1395 — dmidecode bug fix update

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

The dmidecode package provides utilities for extracting x86 and Intel Itanium hardware information from the system BIOS or EFI (Extensible Firmware Interface), depending on the SMBIOS/DMI standard. This information typically includes system manufacturer, model name, serial number, BIOS version, and asset tag, as well as other details, depending on the manufacturer.

BZ#744690

Previously, extended records for Memory Device (DMI type 17) and Memory Array Mapped Address (DMI type 19) DMI types 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.

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

1.42. dovecot

1.42.1. RHSA-2011:0600 — Moderate: dovecot security and enhancement update

Updated dovecot packages that fix two security issues and add one enhancement are now available for Red Hat Enterprise Linux 6.

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

Dovecot is an IMAP server for Linux, UNIX, and similar operating systems, primarily written with security in mind.

Security Fixes

CVE-2010-3780

A flaw was found in the way Dovecot handled SIGCHLD signals. If a large amount of IMAP or POP3 session disconnects caused the Dovecot master process to receive these signals rapidly, it could cause the master process to crash.

CVE-2010-3707

A flaw was found in the way Dovecot processed multiple Access Control Lists (ACL) defined for a mailbox. In some cases, Dovecot could fail to apply the more specific ACL entry, possibly resulting in more access being granted to the user than intended.

Enhancement

BZ#637056

This erratum upgrades Dovecot to upstream version 2.0.9, providing multiple fixes for the "dsync" utility and improving overall performance. Refer to the "/usr/share/doc/dovecot-2.0.9/ChangeLog" file after installing this update for further information about the changes.

Users of dovecot are advised to upgrade to these updated packages, which resolve these issues and add this enhancement. After installing the updated packages, the dovecot service will be restarted automatically.

1.42.2. RHSA-2011:1187 — Moderate: dovecot security update

Updated dovecot 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.

Dovecot is an IMAP server for Linux, UNIX, and similar operating systems, primarily written with security in mind.

Security Fix

CVE-2011-1929

A denial of service flaw was found in the way Dovecot handled NULL characters in certain header names. A mail message with specially-crafted headers could cause the Dovecot child process handling the target user's connection to crash, blocking them from downloading the message successfully and possibly leading to the corruption of their mailbox.

Users of dovecot are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the dovecot service will be restarted automatically.

1.43. dracut

1.43.1. RHBA-2011:0523 — dracut bug fix and enhancement update

Updated dracut packages that fix several bugs and add some enhancements 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 Fixes

BZ#595096

When attempting to boot with MD RAID, udev issued error messages about a missing label because dracut was in the process of rewriting the udev rules files while udev attempted to parse them. dracut now creates temporary rules files, and creates a file for udev's use when the file is considered complete.

BZ#610466

Running **mkinitrd** alone does not override an existing **initramfs** image. When this is attempted, the message stated that the **--force** parameter should be used, but **mkinitrd** only supported the short version **-f** of this parameter. **--force** was added to **mkinitrd** as the long version.

BZ#626389

When booting an IMSM/ISW RAID with dmraid, the mdadm package must be added to a system that has a kickstart minimal install with the **noiswmd** or **rd_NO_MDIMSM** parameters specified.

BZ#630911

When multipath is configured to use user-friendly names, it stores the binding between the wwid and the alias in **/etc/multipath/bindings**. multipath uses this file in **initramfs** when creating devices during early boot, and in the root file system during normal operation. These files were not synchronized during **initramfs** creation, which resulted in naming conflicts that prevented new multipath devices from being created after boot. To work around this, the bindings for the devices in **/etc/multipath/bindings** must be included in the **initramfs**. This can be done by running **dracut -f**.

BZ#636668

dracut did not include all multipath configuration files needed for multipath to include the root device in the multipath listing. dracut now copies over the entire **/etc/multipath** directory to the **initramfs**.

BZ#640979

dracut used all network configuration parameters from the kernel command line, but did not honor any configuration settings in the iBFT. dracut now parses the iBFT settings to set up the network if the **ip=ibft** parameter is specified on the kernel command line.

BZ#642083

dracut did not include multipath in the generated generic **initramfs**, if the host on which it was running had no multipath root device. multipath support is now added to the **initramfs** unconditionally.

BZ#645799

Previously, dracut had a hard-wired dependency on vconfig; this dependency is no longer required, and has been removed.

BZ#650959

When operating with LVM snapshot volumes, I/O errors could occur because the udev rules in the **initramfs** did not exclude those volumes and kept them busy. The udev rules in the **initramfs** were updated to honor the **DM_UDEV_DISABLE_OTHER_RULES_FLAG**, which fixes this issue.

BZ#669438

cryptsetup was required to perform verification when a system attempted to run in FIPS mode. However, the verification check failed because several checksum files were missing from **initramfs**, which resulted in all encrypted devices not being activated. The missing checksum files have been replaced, and this issue no longer occurs. Note however that the dracut-fips must be installed at **initramfs** creation time.

BZ#674238

When multipath ran in the **initramfs** with user_friendly_names set, if it did not find existing mappings in **/etc/multipath/bindings**, it created new mappings. These mappings could conflict with the user_friendly_names set in the normal filesystem's **/etc/multipath/bindings** file. dracut now starts the multipathd daemon with the new **-B** option so that multipath treats the initial bindings file as read-only.

BZ#675118

The **USE_BIOSDEVNAME** variable in the **parse-biosdevname.sh** script was not initialized correctly, which caused an unexpected operator error. This issue was discovered and corrected during development, and did not occur in any production system in the field.

BZ#676018

If a user started dracut with the **-l** or **--local** parameter, or set the dracut base directory via the **dracutbasedir** environment variable, dracut wrote its log to **/tmp/dracut.log**, which could possibly allow local users to overwrite arbitrary files that were writable to the user running dracut, via a symlink attack. dracut now stores the logfile in **$HOME/dracut.log**, when in **-l** or **--local** mode, if **/var/log/dracut.log** is not writeable.

BZ#678294

The **/var/log/dracut.log** file was not created automatically, preventing dracut from writing its logs. dracut now creates its log files if they do not exist.

BZ#691419

The **boot** parameter did not work when the machine was booted in FIPS mode, resulting in numerous mount errors, failed FIPS integrity tests, and dracut refusing to continue. This issue has been corrected, and the **boot** parameter can now be used to specify a boot device, as expected.

BZ#692843

If FIPS mode is enabled and the root partition is encrypted, **/boot** must reside on a non-encrypted, plain (no LVM or RAID) partition, which can be specified with **boot=<boot partition>** as a boot option on the kernel command line.

BZ#692939

After installing to a remote logical unit via Fibre Channel over Ethernet (FCoE), the root device could not be found, resulting in kernel panic. This occurred because the MAC address and interface for the FCoE device was not defined correctly. Installing to a remote logical unit via FCoE now works.

BZ#696131

The **fips.sh** script did not wait for the boot drive to be created, which resulted in an error because the file system type did not exist yet. This has been corrected, and the script now waits for the boot drive to be identified.

Enhancements

BZ#634013

Previously all information about the network interfaces to boot from was read from the kernel command line. dracut was extended to use network interface configuration from the OptionROM, if **fcoe=edd:nodcb** or **fcoe=edd:dcb** is specified on the kernel command line. **ifname=** is not needed in this case.

BZ#645648

dracut has 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.

BZ#670925

dracut now includes the kernel module aes-xts in the **initramfs**, adding support for FIPS-140.

BZ#677340

A new module, dracut-caps has been added to let users omit selected dracut capabilities, and set one or more sysctl parameters.

BZ#689694

Support has been added for the Emulex Tiger Shark adapter for iSCSI.

BZ#692781

Support for several Broadcom drivers (bnx2, bnx2x and bnx2i) has been added to dracut-network.

All users of dracut are advised to upgrade to these updated packages, which resolve these issues.

1.43.2. RHEA-2011:1366 — dracut enhancement update

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

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

Enhancement

BZ#728549

The dm-mod and dm-crypt kernel modules were missing from the list of kernel modules which are pre-loaded for the FIPS-140 (Federal Information Processing Standards) check. With this update, these modules have been added to the list. This update also introduces the dracut-fips-aesni subpackage which should be installed if the aesni-intel module is used in FIPS mode.

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

1.44. e2fsprogs

1.44.1. RHBA-2011:0702 — e2fsprogs bug fix and enhancement update

Updated e2fsprogs packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The e2fsprogs packages contain a number of utilities that create, check, modify, and correct inconsistencies in second extended (ext2) file systems. This includes e2fsck (which repairs file system inconsistencies after an unclean shut down), mke2fs (which initializes a partition to contain an empty ext2 file system), tune2fs (which modifies file system parameters), and most of the other core ext2fs file system utilities.

Bug Fixes

BZ#599338

The e2fsprogs package appeared to contain several regressions because of a number of type-punning issues caused by flags used during the process of building Red Hat Enterprise Linux. Additionally, e2fsprogs had a dependency on libcom_err that was not linked to a specific version of libcom_err. A specific version has been defined to prevent interoperability issues between packages.

BZ#631593

The badblocks command aborted with the error "badblocks: File too large while trying to determine device size" when attempting to run on a 16TB file system. This was caused by a bug in the badblocks command, which this bug fixes, resolving the issue.

BZ#654093

A device that is exactly 16T in size was too large to be opened by the resize2fs utility and attempting to resize some large file systems may remove the resize inode feature if no reserved blocks were left after the operation. This resulted in resize2fs to fail on that device, and resizing a file system close to 16T could remove the resize inode, making further resizing impossible. This patch treats 16T file systems as 16T - 4k, as mkfs does, allowing them to be manipulated by the resize2fs utility, resulting in ext3 and ext4 file systems now able to be resized on devices exactly 16T in size. Do not, however, remove resize inode even if 0 reserved blocks remain, so that subsequent downward resizes are still possible.

BZ#643390

When a value greater than INT_MAX (2147483647) was specified as the argument to mke2fs -G <number of groups>, the command did not complete. This was because the argument for int_log2() was "int", therefore when a value exceeding INT_MAX is specified for the -G option, the value of "arg"

overflows. Also, e2fsprogs only supports 2^32 block file systems so asking for anything greater cannot be honored. Therefore, this patch rejects a number that overflows, and restricts it to INT_MAX+1 so the result does not wrap. This resolves the issue.

BZ#653234

The filefrag command occasionally returned an incorrect number of extensions, returning 0 instead of 1 when using the -v extension. In this patch, special-casing the number of extensions returned in verbose mode and skipping the printing of the header for columns resolves this issue.

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

1.45. ebtables

1.45.1. RHEA-2011:0556 — ebtables enhancement update

An updated ebtables package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

Ethernet bridge tables is a firewalling tool to transparently filter network traffic passing a bridge. The filtering possibilities are limited to link layer filtering and some basic filtering on higher network layers.

Enhancement

BZ#642394

Auditing support is added to create a kernel audit record that records the information flow between a host, guest, and other network entities.

All users requiring firewalling for Ethernet bridge tables are advised to upgrade to this updated package, which adds this enhancement.

1.46. eclipse

1.46.1. RHSA-2011:0568 — Low: eclipse security, bug fix, and enhancement update

Updated eclipse packages that fix one security issue, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. 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 Eclipse software development environment provides a set of tools for C/C++ and Java development.

Security Fix

CVE-2010-4647

A cross-site scripting (XSS) flaw was found in the Eclipse Help Contents web application. An attacker could use this flaw to perform a cross-site scripting attack against victims by tricking them into visiting a specially-crafted Eclipse Help URL.

The following Eclipse packages have been upgraded to the versions found in the official upstream Eclipse Helios SR1 release, providing a number of bug fixes and enhancements over the previous versions:

- eclipse-linuxprofilingframework to 0.6.1. (BZ#669461)
- eclipse to 3.6.1. (BZ#656329)
- eclipse-cdt to 7.0.1. (BZ#656333)
- eclipse-birt to 2.6.0. (BZ#656391)
- eclipse-emf to 2.6.0. (BZ#656344)
- eclipse-gef to 3.6.1. (BZ#656347)
- eclipse-mylyn to 3.4.2. (BZ#656337)
- eclipse-rse to 3.2. (BZ#656338)
- eclipse-dtp to 1.8.1. (BZ#656397)
- eclipse-changelog to 2.7.0. (BZ#669499)
- eclipse-valgrind to 0.6.1. (BZ#669460)
- eclipse-callgraph to 0.6.1. (BZ#669462)
- eclipse-oprofile to 0.6.1. (BZ#670228)

In addition, the following updates were made to the dependencies of the Eclipse packages above:

- jetty-eclipse to 6.1.24. (BZ#661845)
- icu4j to 4.2.1. (BZ#656342)
- sat4j to 2.2.0. (BZ#661842)
- objectweb-asm to 3.2. (BZ#664019)

Bug Fixes

BZ#622713

Incorrect URIs for GNU Tools in the "Help Contents" window have been fixed.

BZ#622867

The profiling of binaries did not work if an Eclipse project was not in an Eclipse workspace. This update adds an automated test for external project profiling, which corrects this issue.

BZ#668890

Running a C/C++ application in Eclipse successfully terminated, but returned an I/O exception not related to the application itself in the Error Log window. With this update, the exception is no longer returned.

BZ#669819

The eclipse-mylyn package showed a "20100916-0100-e3x" qualifier. The qualifier has been modified to "v20100902-0100-e3x" to match the upstream version of eclipse-mylyn.

BZ#673174

Installing the eclipse-mylyn package failed and returned a "Resource temporarily unavailable" error message due to a bug in the packaging. This update fixes this bug and installation now works as expected.

BZ#678364

Building the eclipse-cdt package could fail due to an incorrect interaction with the local file system. Interaction with the local file system is now prevented and the build no longer fails.

BZ#679543

The libhover plug-in, provided by the eclipse-cdt package, used binary data to search for hover topics. The data location was specified externally as a URL which could cause an exception to occur on a system with no Internet access. This update modifies the plug-in so that it pulls the needed data from a local location.

Enhancements

The Eclipse IDE and Java Development Tools (JDT)

```
- rojects and folders can filter out resources in the workspace.
- new virtual folder and linked files support.
- the full set of UNIX file permissions is now supported.
- addition of the stop button to cancel long-running wizard tasks.
- Java editor now shows multiple quick-fixes via problem hover.
- new support for running JUnit version 4 tests.
- over 200 upstream bug fixes.
```

The Eclipse C/C++ Development Tooling (CDT)

```
- new Codan framework has been added for static code analysis.
- refactoring improvements such as stored refactoring history.
- compile and build errors now highlighted in the build console.
- switch to the new DSF debugger framework.
- new template view support.
- over 600 upstream bug fixes.
```

Users of eclipse should upgrade to these updated packages, which correct these issues and add these enhancements.

1.47. ecryptfs-utils

1.47.1. RHSA-2011:1241 — Moderate: ecryptfs-utils security update

Updated ecryptfs-utils packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

eCryptfs is a stacked, cryptographic file system. It is transparent to the underlying file system and provides per-file granularity. eCryptfs is released as a Technology Preview for Red Hat Enterprise Linux 5 and 6.

The setuid mount.ecryptfs_private utility allows users to mount an eCryptfs file system. This utility can only be run by users in the "ecryptfs" group.

Security Fixes

CVE-2011-1831

A race condition flaw was found in the way mount.ecryptfs_private checked the permissions of a requested mount point when mounting an encrypted file system. A local attacker could possibly use this flaw to escalate their privileges by mounting over an arbitrary directory.

CVE-2011-1832

A race condition flaw in umount.ecryptfs_private could allow a local attacker to unmount an arbitrary file system.

CVE-2011-1834

It was found that mount.ecryptfs_private did not handle certain errors correctly when updating the mtab (mounted file systems table) file, allowing a local attacker to corrupt the mtab file and possibly unmount an arbitrary file system.

CVE-2011-1835

An insecure temporary file use flaw was found in the ecryptfs-setup-private script. A local attacker could use this script to insert their own key that will subsequently be used by a new user, possibly giving the attacker access to the user's encrypted data if existing file permissions allow access.

CVE-2011-1837

A race condition flaw in mount.ecryptfs_private could allow a local attacker to overwrite arbitrary files.

CVE-2011-3145

A race condition flaw in the way temporary files were accessed in mount.ecryptfs_private could allow a malicious, local user to make arbitrary modifications to the mtab file.

CVE-2011-1833

A race condition flaw was found in the way mount.ecryptfs_private checked the permissions of the directory to mount. A local attacker could use this flaw to mount (and then access) a directory they would otherwise not have access to. Note: The fix for this issue is incomplete until a kernel-space change is made. Future Red Hat Enterprise Linux 5 and 6 kernel updates will correct this issue.

Red Hat would like to thank the Ubuntu Security Team for reporting these issues. The Ubuntu Security Team acknowledges Vasiliy Kulikov of Openwall and Dan Rosenberg as the original reporters of CVE-2011-1831, CVE-2011-1832, and CVE-2011-1833; Dan Rosenberg and Marc Deslauriers as the original reporters of CVE-2011-1834; Marc Deslauriers as the original reporter of CVE-2011-1835; and Vasiliy Kulikov of Openwall as the original reporter of CVE-2011-1837.

Users of ecryptfs-utils are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

1.48. edac-utils

1.48.1. RHBA-2011:0768 — edac-utils bug fix and enhancement update

Updated edac-utils packages that fix one bug and add one enhancement are now available for Red Hat Enterprise 6.

EDAC is the current set of drivers in the Linux kernel that handles detection of ECC errors from memory controllers for most chipsets on the x86, AMD64, and Intel 64 architectures. The user-space component consists of an initscript which ensures that EDAC drivers and DIMM labels are loaded at system startup, as well as a library and utility for reporting current error counts from the EDAC sysfs files.

Bug Fix

BZ#632665

Previously, the edac-utils initscript did not use the standard error codes of other initscripts because several mandatory actions were missing. This update implements the initscript actions "condrestart", "try-restart", "force-reload" and sets the return values for each action accordingly. Now, the initscript uses the standard error code.

Enhancement

BZ#640113

This update extends the maximum number of channels from 2 to 6, in order to allow it to work with some designs that have 4 channels on FB-DIMM motherboards, e.g. the ones with Intel 7300 chipset. By default, this update identifies the motherboard via BIOS DMI board information. If not available, it will fallback to use DMI system information.

Note: the improvements from upstream version 0.16 are now added to edac-utils, including new motherboard labels, an option to delay the motherboard write labels, and a better parser to retrieve memory and vendor information from the system.

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

1.49. efibootmgr

1.49.1. RHBA-2011:0674 — efibootmgr bug fix update

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

The efibootmgr utility is responsible for the boot loader installation on Unified Extensible Firmware Interface (UEFI) systems.

Bug Fix

BZ#612280

Due to missing support for 4KB disk sectors, an attempt to use the efibootmgr utility to create a boot option on such a device caused the utility to fail with the following error message:

```
Error: no partition information on disk [device].
Cowardly refusing to create a boot option.
```

This update adapts the efibootmgr utility to provide support for 4KB disk sectors, resolving this issue.

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

1.50. elfutils

1.50.1. RHBA-2011:0578 — elfutils bug fix update

Updated elfutils packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

The elfutils package contains utilities and libraries for working with compiled binary files. Its libraries are used by the SystemTap instrumentation system found in the systemtap package.

Bug Fix

BZ#652858

After prelink had been run on the system, using SystemTap user-space probes that targeted functions or statements in certain shared libraries, or executables based on a separate debuginfo file, caused resolution to the wrong PC location in a linked binary. As a result, the intended probes failed to fire at the correct place in the program, which could have caused the program to crash or misbehave due to a corrupted instruction sequence resulting from incorrect breakpoint insertions. With this update, the libdwfl library code (the libdw.so shared object library) was adjusted to use a more reliable method of compensating for prelink's effect on the address layout of a binary when aligning a runtime PC address with an address computed separately from the separated debuginfo file. SystemTap probes should now work the same on prelinked binaries as they would on binaries that have not been prelinked.

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

1.51. emacs

1.51.1. RHBA-2011:0717 — emacs bug fix update

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

GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (elisp), and the capability to read email and news.

Bug Fixes

BZ#612385

Prior to this update, Emacs incorrectly displayed Japanese documents using JIS X 0213:2004 (JIS2004) compliant fonts, even though other parts of the system prefer and use older fonts. This update lowers the priority of JIS X 0213:2004 to ensure the consistent use of fonts in the system.

BZ#613759

Previously, the emacs packages required the aspell and hunspell spell checkers to be installed. Since the use of a spell checker is completely optional, this update removes aspell and hunspell from the list of dependencies, so that Emacs can now be installed without these packages.

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

1.52. epydoc

1.52.1. RHBA-2011:0316 — epydoc bugfix update

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

Epydoc is a tool for generating API documentation for Python modules, based on their docstrings. A lightweight markup language called epytext can be used to format docstrings, and to add information about specific fields, such as parameters and instance variables. Epydoc also understands docstrings written in ReStructuredText, Javadoc and plaintext.

Bug Fix

BZ#657567

Previously, the summary extractor of reStructuredText did not work properly and the documentation process failed. Due to this behavior, building packages could fail. This update resolves this problem. Packages now build successfully.

All users of epydoc are advised to upgrade to this updated package, which resolves this issue.

1.53. evolution

1.53.1. RHBA-2011:0714 — evolution bug fix update

Updated evolution packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

Evolution is the GNOME email, calendar, contact management and communications application. The components which make up Evolution are tightly integrated with one another and act as a seamless personal information-management (PIM) tool.

Bug Fixes

BZ#696881

When a user tried to migrate their mail folder settings after upgrading to Red Hat Enterprise Linux 6, or restore a backup from the previous version of Evolution, Evolution sometimes terminated unexpectedly. This bug has been fixed and no longer occurs during the migration process.

BZ#585931

When a user created or edited a task in Evolution, the tooltip for the print icon in the toolbar was missing. This tooltip has been added and is now correctly displayed when hovering over the print icon.

BZ#628964

When printing the "Day" view of a calendar in Evolution to a Postscript file, the selected day and month name overlapped the line below. The issue has been resolved; overlaps no longer take place.

BZ#632968

When a user selected the "Submit bug report" option in the "Help" menu, a spurious "Bug Buddy is not installed" error message appeared. Because Bug Buddy is not a component of Red Hat Enterprise Linux 6, the menu option to submit a bug was removed.

BZ#633600

When creating a mail account in the Evolution Account Assistant using the POP protocol, the keyboard shortcut for "Delete after 7 days" (Alt+D) did not work. With this update, the GUI widget accepts the keyboard shortcut for the "Delete after 7 days" functionality and entering the shortcut now works as expected.

BZ#633629

The "Create a Memo" item from the "Message" menu was active when it was not supposed to be. As a consequence, Evolution terminated unexpectedly when the user selected this item. With this update, the "Create a Memo" item is deactivated when it is supposed to be, with the result that the user can no longer crash Evolution by selecting it.

BZ#666875

When viewing an email message larger than the maximum value defined in the settings Edit -> Preferences -> Mail Preferences -> "Do not format messages when text size exceeds [n KB]" caused Evolution to terminate unexpectedly. This bug has been fixed and viewing a message larger than the set value no longer causes Evolution to crash.

BZ#667083

When a user created a calendar meeting in Evolution with at least 16 attendees and right-clicked "Reply to all", the application terminated unexpectedly sometimes. The problem was with the reallocation of memory in glib2 and it has been fixed. Replying to all attendees of a calendar meeting now works as expected.

BZ#633189

When a user clicked into the input field under the Summary header in Task or Memo section in Evolution, and switched its input method to any language managed by ibus (such as Chinese), foreign characters could not be entered. The fix involves calling some functions in the correct order so the events for the input method are registered properly.

BZ#628882, BZ#630316, BZ#632998, BZ#638643

When using one of four Asian locales (ml_IN, hi_IN, ta_IN, zh_TW), the following problems occurred in Evolution Assistant: differing translations for the label and button "Forward" and "Finish", a missing and erroneous translation for the "Forward" label, and the ZWJ/ZWNJ characters visible by mistake. With this update, corrected translations has been provided.

BZ#633181

In the "Evolution Appointment" dialog, when using the Chinese Simplified locale (zh_CN), there was an erroneous translation on the "for" button. The translation has been modified and Evolution now displays a proper button text translation.

Users are advised to upgrade to these updated packages, which fix these bugs and correct several localization issues.

1.54. evolution-data-server

1.54.1. RHBA-2011:0713 — evolution-data-server bug fix update

An updated evolution-data-server package that fixes several bugs is now available.

The evolution-data-server package provides a unified back end for applications which interact with contacts, task and calendar information. Evolution Data Server was originally developed as a back end for Evolution, but is now used by various other applications.

This updated evolution-data-server package provides fixes for the following bugs:

- cannot enter date in New->Appointment dialog with or_IN language (BZ#629919)
- crash when using Google address book (BZ#634949)
- folder unread count doesn't update properly on search folders (BZ#657117)
- crash when receiving On The Web calendar items (BZ#660356)
- crash when adding contact to a contact list (BZ#666879)

Users are advised to upgrade to this updated evolution-data-server package, which resolves these issues.

1.55. evolution-mapi

1.55.1. RHBA-2011:0800 — evolution-mapi bug fix update

An updated evolution-mapi package that fixes a crash is now available for Red Hat Enterprise Linux 6.

The MAPI extension for Evolution (evolution-mapi) allows Evolution to interact with MS Exchange 2007 servers.

Bug Fix

BZ#66642

When accessing an address book on an Exchange 2007 server, a flaw in the MAPI extension caused the evolution-data-server process to occasionally crash. This was because evolution-mapi mistook EDataBookView as a GObject, instead of a bonobo_object, and as a result was reffing/unreffing it with g_object_ref/g_object_unref. This patch uses the proper functions for ref/unref, resolving the issue.

Users are advised to upgrade to this updated evolution-mapi package, which fixes this problem.

1.56. fakechroot

1.56.1. RHBA-2011:0719 — fakechroot bug fix update

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

The fakechroot utility allows a user to run programs in an environment that enables the use of the chroot command without the need for root privileges.

Bug Fix

BZ#598451

Prior to this update, the fakechroot packages were marked as multilib, which allowed users to install these packages for multiple architectures at the same time. However, this feature is not fully supported by fakechroot. Since the 32-bit version of is not actually needed, this update adds the

"ExclusiveArch: x86-64" tag to the RPM spec file, so that the fakechroot packages are now available only for the 64-bit x86 architecture.

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

1.56.2. RHBA-2011:1218 — fakechroot bug fix update

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

The fakechroot utility lets you run programs in a fake chroot environment without superuser privileges.

Bug Fix

BZ#730647

Due to multilib problems, the fakeroot command was only built on 64-bit architectures as a workaround, one which prevented the RPM package from being built on other architectures. This update resolves the multilib problems so that fakeroot now builds successfully on all architectures.

All users of fakechroot should upgrade to these updated packages, which fix this bug.

1.57. fcoe-utils

1.57.1. RHBA-2011:0743 — fcoe-utils bug fix update

An updated fcoe-utils package that fixes several bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The fcoe-utils package allows users to use Fibre Channel over Ethernet (FCoE). The package contains the fcoeadm command line tool for configuring FCoE interfaces, and the fcoemon service to configure DCB (Data Center Bridging) Ethernet QoS filters.

The fcoe-utils package has been upgraded to upstream version 1.0.18, which provides a number of bug fixes and enhancements over the previous version. (BZ#672453, BZ#691613)

Bug Fixes

BZ#645917

Previously, in a particular setup with multipath and FCoE services, the system sometimes became unresponsive during shutdown or reboot, and a hard reboot was required to get the system back up. Now, an additional FCoE root filesystem check has been added to the init script and the system no longer hangs during reboot or shutdown in this scenario.

BZ#658076

Sometimes, FCoE devices are not discovered immediately by the system. As a consequence, some FCoE partitions were previously not automounted after a boot. With this update, the FCoE init script waits for a certain amount of time (65 seconds by default), which is enough for most FCoE partitions to be discovered and mounted during the boot.

BZ#678487

Running the fcoeadm tool without the FCoE stack loaded caused the fcoeadm tool to terminate with a backtrace when it tried to free an unallocated pointer. With this update, only successfully allocated pointers are freed and the fcoeadm tool returns a proper error message otherwise.

BZ#689631

After VLAN discovery was tried unsuccessfully 10 times, the default FCoE driver for an interface was used instead of the preferred one. With this update, VLAN discovery is retried indefinitely and FCoE interfaces are now created only upon VLAN discovery, with proper drivers.

BZ#623567

For several fcoe-utils executables, there were minor inconsistencies in the documentation between their command help output and their man pages. With this update, the documentation has been updated and the man pages and help output are now consistent.

BZ#645796

The vconfig package had been marked for removal from the distribution, but the fcoe-utils package required it at runtime. With this update, this dependency has been removed in favor of the iproute package.

BZ#680578

When an FCoE VLAN interface was restarted, the FCoE interface was not re-enabled after the VLAN interface was brought up again. This bug has been fixed and the FCoE interface is now automatically enabled after the VLAN interface is brought up.

Enhancement

BZ#669211

With this update, the fcoe-utils package introduces a new SUPPORTED_DRIVERS configuration option to list all the low-level drivers that can potentially claim a network device. The package also uses the new sysfs module path introduced by the Red Hat Enterprise Linux 6.1 kernel update.

Users of fcoe-utils are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

1.58. febootstrap

1.58.1. RHEA-2011:0587 — febootstrap enhancement update

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

febootstrap is used to create a basic Red Hat Enterprise Linux or Fedora filesystem, and builds initramfs (initrd.img) or filesystem images.

The febootstrap packages have been upgraded to upstream version 2.11, which provides a number of bug fixes and one enhancement over the previous version. (BZ#628849)

Enhancements

BZ#669839

This update provides the subpackage febootstrap-supermin-helper for the runtime helper program. Now, libguestfs runtime depends only on febootstrap-supermin-helper, which reduces the dependencies.

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

1.59. fence-agents

1.59.1. RHBA-2011:0745 — fence-agents bug fix and enhancement update

An updated fence-agents package that fixes bugs, adds support for new hardware and Red Hat Enterprise Virtualization 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 Fixes

BZ#618703, BZ#623266

Metadata generation has been corrected in order to provide information for all known parameters for each fencing agent.

BZ#619096

Port is now a synonym of module_name for fence_drac5, making it consistent with other fencing agents.

BZ#648892

Information on how to use fence_ipmi with HP iLO version 3 has been added to the manual page.

BZ#635824

The fence_egenera manual page has been improved.

BZ#640343

fence_scsi now works when devices report "Unit Attention".

BZ#644385

fence_scsi now verifies action results.

BZ#644389

fence_scsi now correctly identifies device mapper multipath devices.

BZ#670910

fence_scsi pattern matching has been improved.

BZ#672597

fence_scsi now logs errors whenever a command fails.

Enhancements

BZ#580492, BZ#678904

Support for Cisco UCS blade systems is now provided.

BZ#614046

It is now possible for one node to delay fencing in a two-node cluster.

BZ#655764

Fence_ipmilan can now use the "diag" option.

BZ#595383

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#642671

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

BZ#642235, BZ#680170

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.

BZ#653504

An issue with fence_scsi where the key was erroneously reported as 0 has been addressed.

BZ#678522

fence_wti now correctly handles large (>20) port switches.

BZ#681669, BZ#681674

fence_rhevm has been updated to the current RHEVM development API.

BZ#682715

fence_cisco_ucs was missing from the fence-agents package, but is now included.

All users requiring any of the changes noted above should upgrade to this new package, which fixes these issues and adds these enhancements.

1.60. fence-virt

1.60.1. RHBA-2011:0731 — fence-virt bug fix and enhancement update

Updated fence-virt packages that provide a bug fix and an enhancement are now available for Red Hat Enterprise Linux 6.

The fence-virt packages provide a fencing agent for virtual machines as well as a host agent which processes fencing requests.

Bug Fix

BZ#667170

The manual pages now correctly refer to "fence_virt.conf" instead of "fence_virtd.conf."

Enhancement

BZ#690582

Fence-virtd now operates with newer versions of QMF.

All users of fence-virt are advised to upgrade to these updated packages, which address these issues.

1.61. file

1.61.1. RHBA-2011:0204 — file bug fix update

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

The file command is used to identify a particular file according to the type of data contained in the file.

Bug Fixes

BZ#594083

Prior to this update, the file utility could be unable to recognize Python scripts correctly. This update improves the file type recognition, and Python scripts are now identified as expected.

BZ#608686

In accordance with POSIX standards, when the file utility is used on a file that does not exist, cannot be read, or is of an unknown type, it returns 0 exit code. This update extends the manual page to document this behavior.

BZ#610795

The file utility has been updated to recognize the WebM media container.

BZ#637782

The file utility has been updated to recognize the ZIP64 file format.

BZ#643046

The file utility has been updated to recognize volume_key escrow packets.

BZ#670125

Due to an error in a magic pattern, the file utility incorrectly identified GFS file systems as GFS2. With this update, the magic pattern has been corrected, and GFS file systems are now identified as expected.

All users of file are advised to upgrade to these updated packages, which resolve these issues.

1.62. fipscheck

1.62.1. RHEA-2011:0672 — fipscheck enhancement update

Updated fipscheck packages which relocate the library from /usr to /lib or /lib64 are now available.

FIPSCheck is a library used to verify the integrity of modules validated under FIPS-140-2. The fipscheck package provides helper binaries for creating and verifying HMAC-SHA256 checksum files.

Enhancement

BZ#669077

The fipscheck library can be linked to binaries (such as cryptsetup) which have to operate when /usr is not mounted. With this update, the fipscheck library relocates from /usr to /lib or /lib64 (depending on the underlying architecture) to allow linking to such binaries.

All fipscheck users are advised to upgrade to these updated packages, which add this enhancement.

1.63. firefox

1.63.1. RHSA-2011:0885 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2011-2377

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-2011-0083, **CVE-2011-0085**, **CVE-2011-2363**

Multiple dangling pointer flaws were found in Firefox. 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-2011-2364, **CVE-2011-2365**, **CVE-2011-2374**, **CVE-2011-2375**, **CVE-2011-2376**

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-2011-2371

An integer overflow flaw was found in the way Firefox handled JavaScript Array objects. A website containing malicious JavaScript could cause Firefox to execute that JavaScript with the privileges of the user running Firefox.

CVE-2011-2373

A use-after-free flaw was 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-2011-2362

It was found that Firefox could treat two separate cookies as interchangeable if both were for the same domain name but one of those domain names had a trailing "." character. This violates the same-origin policy and could possibly lead to data being leaked to the wrong domain.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.18.

Bug Fix

BZ#698313

With previous versions of Firefox on Red Hat Enterprise Linux 5, the "background-repeat" CSS (Cascading Style Sheets) property did not work (such images were not displayed and repeated as expected).

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.18, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.63.2. RHSA-2011:1164 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2011-2982

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-2011-0084

A dangling pointer flaw was found in the Firefox Scalable Vector Graphics (SVG) text manipulation routine. A web page containing a malicious SVG image could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-2378

A dangling pointer flaw was found in the way Firefox handled a certain Document Object Model (DOM) element. 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-2011-2981

A flaw was found in the event management code in Firefox. A website containing malicious JavaScript could cause Firefox to execute that JavaScript with the privileges of the user running Firefox.

CVE-2011-2983

A flaw was found in the way Firefox handled malformed JavaScript. A web page containing malicious JavaScript could cause Firefox to access already freed memory, causing Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-2984

It was found that a malicious web page could execute arbitrary code with the privileges of the user running Firefox if the user dropped a tab onto the malicious web page.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.20.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.20, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.63.3. RHSA-2011:1242 — 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.

It was found that a Certificate Authority (CA) issued a fraudulent HTTPS certificate. This update renders any HTTPS certificates signed by that CA as untrusted, except for a select few. The now untrusted certificates that were issued before July 1, 2011 can be manually re-enabled and used again at your own risk in Firefox; however, affected certificates issued after this date cannot be re-enabled or used. (BZ#734316)

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.

1.63.4. RHSA-2011:1268 — 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.

The RHSA-2011:1242 Firefox update rendered HTTPS certificates signed by a certain Certificate Authority (CA) as untrusted, but made an exception for a select few. This update removes that exception, rendering every HTTPS certificate signed by that CA as untrusted. (BZ#735483)

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.22. After installing the update, Firefox must be restarted for the changes to take effect.

1.63.5. RHSA-2011:1341 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2011-2995

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-2011-2372

A flaw was found in the way Firefox processed the "Enter" keypress event. A malicious web page could present a download dialog while the key is pressed, activating the default "Open" action. A remote attacker could exploit this vulnerability by causing the browser to open malicious web content.

CVE-2011-3000

A flaw was found in the way Firefox handled Location headers in redirect responses. Two copies of this header with different values could be a symptom of a CRLF injection attack against a vulnerable server. Firefox now treats two copies of the Location, Content-Length, or Content-Disposition header as an error condition.

CVE-2011-2999

A flaw was found in the way Firefox handled frame objects with certain names. An attacker could use this flaw to cause a plug-in to grant its content access to another site or the local file system, violating the same-origin policy.

CVE-2011-2998

An integer underflow flaw was found in the way Firefox handled large JavaScript regular expressions. A web page containing malicious JavaScript could cause Firefox to access already freed memory, causing Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.23.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.23, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.63.6. RHSA-2011:1437 — Critical: firefox security update

Updated firefox packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

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

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

Security Fixes

CVE-2011-3647

A flaw was found in the way Firefox handled certain add-ons. A web page containing malicious content could cause an add-on to grant itself full browser privileges, which could lead to arbitrary code execution with the privileges of the user running Firefox.

CVE-2011-3648

A cross-site scripting (XSS) flaw was found in the way Firefox handled certain multibyte character sets. A web page containing malicious content could cause Firefox to run JavaScript code with the permissions of a different website.

CVE-2011-3650

A flaw was found in the way Firefox handled large JavaScript scripts. A web page containing malicious JavaScript could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.24.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.24, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.64. firstaidkit

1.64.1. RHEA-2011:0166 — firstaidkit enhancement update

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

FirstAidKit is a tool that runs automated diagnostics of an installed Red Hat Enterprise Linux system.

Enhancement

BZ#584677

These updated packages introduce a new manual page with an outline of the basic concepts and format of the main configuration file (that is, /etc/firstaidkit/firstaidkit.conf by default). Note that this manual page does not replace a detailed description of available configuration options in the configuration file itself.

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

1.65. firstboot

1.65.1. RHBA-2011:0742 — firstboot bug fix and enhancement update

Updated firstboot packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The firstboot utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.

Bug Fixes

BZ#658869

Previously, no screen was provided to change the root password in firstboot. Due to this lack, users had to change the settings of system-config-users to the root password within the Advanced window of firstboot's create user screen. This update adds a module to change the root password. Now, users can view a set the root password in firstboot, if run with the option "the --reconfig".

BZ#659451

Previously, users could not skip the user creation screen. Due to this lack, users had to create a user account with an UID number above or equal to 500 to continue to the next step of the first boot process. With this update, the check for valid user accounts in the system checks whether a user account with a valid login shell is present and not only user accounts with an UID number above or equal to 500. If there's no such user account present firstboot shows a warning, but allows the user to go to the next step. Now, users can skip the user creation part of firstboot.

Enhancement

BZ#463564

Previously, the firstboot utility did not run automatically after installation on IBM's System/390 architecture. Due to this issue, users had to run firstboot manually. This update adds automatic execution. Now, the firstboot utility runs automatically when the root user logs in to the system for the first time with a capable terminal.

All firstboot users are advised to upgrade to these updated packages, which fix these bugs and adds this enhancement.

1.66. foomatic

1.66.1. RHSA-2011:1110 — Moderate: foomatic security update

An updated foomatic 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.

Foomatic is a comprehensive, spooler-independent database of printers, printer drivers, and driver descriptions. The package also includes spooler-independent command line interfaces to manipulate queues and to print files and manipulate print jobs. foomatic-rip is a print filter written in C.

Security Fix

CVE-2011-2964

An input sanitization flaw was found in the foomatic-rip print filter. An attacker could submit a print job

with the username, title, or job options set to appear as a command line option that caused the filter to use a specified PostScript printer description (PPD) file, rather than the administrator-set one. This could lead to arbitrary code execution with the privileges of the "lp" user.

All foomatic users should upgrade to this updated package, which contains a backported patch to resolve this issue.

1.67. freeradius

1.67.1. RHBA-2011:0610 — freeradius bug fix and enhancement update

Updated freeradius packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

FreeRADIUS is an open source RADIUS server which allows RADIUS clients to perform authentication against the RADIUS server. The RADIUS server may optionally perform accounting of it's operations via the RADIUS protocol.

The FreeRADIUS packages have been upgraded to upstream version 2.1.10, which provides a number of bug fixes over the previous version. (BZ#644100)

Bug Fixes

BZ#689045

Previously, the FreeRADIUS server failed to start when the rlm_perl or rlm_python modules were used due to unresolved symbols encountered by the dynamic loader. This update uses the dynamic loader option which must be explicitly turned on via lt_dladvise to allow loaded modules to globally export their symbols. Now, rlm_perl and rlm_python FreeRADIUS modules are successfully loaded and the FreeRADIUS server successfully starts in this configuration.

Enhancement

BZ#599528

This update makes the radtest script available for testing with IPv6.

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

1.68. freetype

1.68.1. RHSA-2011:1085 — Important: freetype security update

Updated freetype 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.

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.

Security Fix

CVE-2011-0226

A flaw was found in the way the FreeType font rendering engine processed certain 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.

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.

1.68.2. RHSA-2011:1402 — Important: freetype security update

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

The Red Hat Security Response Team has rated this update as having 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.

Security Fix

CVE-2011-3256

Multiple input validation flaws were found in the way FreeType processed bitmap font files. If a specially-crafted font file was loaded by an application linked against FreeType, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Note: These issues only affected the FreeType 2 font engine.

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

1.68.3. RHSA-2011:1455 — Important: freetype security update

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

The Red Hat Security Response Team has rated this update as having 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.

Security Fix

CVE-2011-3439

Multiple input validation flaws were found in the way FreeType processed CID-keyed fonts. If a specially-crafted font file was loaded by an application linked against FreeType, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Note: These issues only affected the FreeType 2 font engine.

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

1.69. fuse

1.69.1. RHSA-2011:1083 — Moderate: fuse security update

Updated fuse packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

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

FUSE (Filesystem in Userspace) can implement a fully functional file system in a user-space program. These packages provide the mount utility, fusermount, the tool used to mount FUSE file systems.

Security Fix

CVE-2010-3879, **CVE-2011-0541**, **CVE-2011-0542**, **CVE-2011-0543**

Multiple flaws were found in the way fusermount handled the mounting and unmounting of directories when symbolic links were present. A local user in the fuse group could use these flaws to unmount file systems, which they would otherwise not be able to unmount and that were not mounted using FUSE, via a symbolic link attack.

Note: The util-linux-ng RHBA-2011:0699 update must also be installed to fully correct the above flaws.

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

1.70. gcc

1.70.1. RHBA-2011:0663 — gcc bug fix update

A gcc update that resolves several compiler bugs is now available for Red Hat Enterprise Linux 6.

The gcc packages include C, C++, Java, Fortran, Objective C, Objective C++ and Ada 95 GNU compilers, along with related support libraries.

Bug Fixes

BZ#630166

These updated packages provide support for the "-mcmodel=medium" and "-mcmodel=large" options on the 64-bit PowerPC architecture. These new options provide the ability to extend the TOC addressing space up to 2GB.

BZ#632366

gcc now has the ability to emit pre-fetch instructions for "memcmp", "memcpy" and "memset" in-line expansions when optimizing for IBM System z10 CPUs.

BZ#624889

Previously, leaf functions that accessed TLS variables in the global or local dynamic model were not generating a large enough stack frame on PowerPC 64-bit. In this updated package, the generated stack frame is now larger than 112 bytes, resolving this issue.

BZ#675132

Previously a regression in the gfortran compiler was causing the "-M" option to not be recognized. In these updated packages the "-M" option is now recognized and functions as expected.

BZ#592502

Previously, the optimizations performed when calculating induction variables during the induction variable optimization (ivopts) pass were not as efficient as previous releases. In these updated packages, the optimizations performed during the induction variable optimization (ivopts) pass is improved.

BZ#618258

Previously, if a Java application built with gcj attempted to submit a print job to a print queue that was disabled, the process would enter a busy loop. This update fixes this issue by first checking if the print queue is null before attempting to send it a print job.

BZ#659582

Previously, using "always_inline" on a function when compiling with "-g" without any "-O" options would cause the compiler to insert debugging annotations in unexpected locations. Consequently, the unexpected annotations caused the compiler to crash with an internal error. In these updated packages, the compiler is modified to properly handle attributes which change optimization levels, such as always_inline, properly.

BZ#632370

This update provides code optimizations for the IBM System z architecture.

BZ#635015

The mask operand for the AVX mask load/store is fixed.

All users of gcc are advised to upgrade to these updated packages which address these issues.

1.71. gdb

1.71.1. RHBA-2011:0638 — gdb bug fix and enhancement update

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

The GNU debugger, gdb, is a debugger for programs written in C, C++, and other languages.

The gdb package has been upgraded to upstream version 7.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#649030)

Bug Fixes

BZ#611435

GDB crashed when reading a kernel core dump file because the value of temporary current inferior process was set to minus_one_ptid (all processes). The value is now set to null_ptid (no processes) and GDB displays the vmcore file.

BZ#625239

When the gcore utility created a core file for an executable compiled with the "-Wl,-z,relro" parameter, GDB was unable to open it. This occurred because the file did not contain the list of shared libraries. Such core files now contain the shared library list and can be opened.

BZ#629236

GDB Python's pretty-printing feature provides an easily-readable view on complex C++ STL data structures. GDB crashed when displaying such structures. This occurred when the pretty printer threw a Python exception and GDB crashed due to a NULL pointer dereference. GDB now displays the easily-readable view of any C++ STL data structure correctly.

BZ#632259

GDB aborted unexpectedly if you set breakpoints on GNU-IFUNC functions and started the debugged program because the breakpoints could not resolve the target functions of the GNU-IFUNC functions at program startup. Breakpoints on GNU-IFUNC functions are now resolved when the program calls the target function.

BZ#636298

With GDB, you can modify VSX registers on PowerPC platforms. Changing some VSX registers corrupted other VSX registers. GDB now sets VSX registers independently.

BZ#639645

GDB aborted unexpectedly when an inferior shared library list changed during an inferior function call. This occurred because GDB reset all breakpoints including the temporary breakpoint, which was created by the call, and attempted to delete the breakpoint again after the call finished. The temporary breakpoint now remains valid during the entire inferior function call.

BZ#639647

GDB could have hung when debugging multithreaded programs with the setuid() function because the siginfo_t information associated with a signal number got lost. GDB now no longer resubmits or reorders signals and the siginfo_t value is preserved.

BZ#661773

GDB terminated unexpectedly after user run the "info program" command because a change of the shared library list corrupted the data in the internal GDB structure "bpstat". The structure now contains correct data even after a change in the shared library list and "info program" works as expected.

BZ#663449

Test suite file break-interp.exp reported for PowerPC platforms several FAIL results. A number of fixes have been applied to address these issues and the test suite for PowerPC now runs successfully.

BZ#682891

GDB crashed when attempting to access dynamic types, such as variable length arrays, using the GDB/MI interface. GDB now no longer crashes under these circumstances.

BZ#688788

On the i686 architecture, the awatch and rwatch commands printed an error when entered before the program-to-be-debugged started. GDB now by default debugs on the native architecture and the commands can be used before the program-to-be-debugged starts.

Enhancements

BZ#562758

Debugged programs may use C++ templates. C++ templates provide template symbols for instantiation of classes and functions. GDB debugged the template instances but the template symbols were not accessible. GDB now displays the template symbols while debugging the template instances.

BZ#609782

Fortran supports array slicing. GDB could not slice multidimensional arrays. GDB now supports slicing of such arrays.

BZ#673696

GDB did not display pthread_t for threads found in the core. GDB now displays pthread_t for the threads.

Users are advised to upgrade to these packages, which resolve the bugs and add the enhancements.

1.72. ghostscript

1.72.1. RHBA-2011:0527 — ghostscript bug fix update

Updated ghostscript packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

The Ghostscript suite provides a PostScript interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language), and an interpreter for PDF files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by most printers and displays. This enables users to display PostScript files and print them on non-PostScript printers.

Bug Fixes

BZ#621118

Previously, including a large JBIG2 compressed image in the PDF input file could cause the pdf2ps conversion utility to terminate unexpectedly with a segmentation fault. This was caused by the fact that the result of the "jbig2_image_new" function call was not always checked properly. This error has been fixed, and the inclusion of JBIG2 images no longer causes pdf2ps to crash.

BZ#629562

Due to incorrect object management, Ghostscript could attempt to read from uninitialized memory, which could lead to a segmentation fault. This update applies a backported patch that addresses this issue, and Ghostscript no longer crashes.

BZ#629941

The Fontmap.local file installed with the ghostscript package allows a system administrator to override font substitutions. However, previous versions of the Ghostscript suite did not use this file at all. This error has been fixed, and the file is now used as expected.

BZ#675692

Previously, using the ps2pdf utility to convert a PostScript file to the PDF format caused the resulting document to be created without working hyperlinks. This update applies an upstream patch that resolves this issue, and ps2pdf now crates PDF files with correct hyperlinks.

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

1.72.2. RHBA-2011:0899 — ghostscript bug fix update

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

The Ghostscript suite provides a PostScript interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language), and an interpreter for PDF files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by most printers and displays. This enables users to display PostScript files and print them on non-PostScript printers.

Bug Fix

BZ#710651

Previously, the default paper size was selected in portrait orientation when printing documents in landscape orientation. Consequently, the output was printed in portrait orientation and the content was cropped on the right side. With this update, if the paper size matches in landscape mode, that paper size is selected and the landscape orientation is selected for printing.

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

1.73. gimp

1.73.1. RHSA-2011:0839 — Moderate: gimp security update

Updated gimp packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

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

The GIMP (GNU Image Manipulation Program) is an image composition and editing program.

Security Fixes

CVE-2010-4543

A heap-based buffer overflow flaw was found in the GIMP's Paint Shop Pro (PSP) image file plug-in. An attacker could create a specially-crafted PSP image file that, when opened, could cause the PSP plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP.

CVE-2010-4540, **CVE-2010-4541**, **CVE-2010-4542**

A stack-based buffer overflow flaw was found in the GIMP's Lightning, Sphere Designer, and Gfig image filters. An attacker could create a specially-crafted Lightning, Sphere Designer, or Gfig filter configuration file that, when opened, could cause the relevant plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP.

Users of the GIMP are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The GIMP must be restarted for the update to take effect.

1.74. glib2

1.74.1. RHBA-2011:0535 — glib2 bug fix update

Updated glib2 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

GLib is a low-level core library that forms the basis for projects such as GTK+ and GNOME. It provides data structure handling for C, portability wrappers, and interfaces for such runtime functionality as an event loop, threads, dynamic loading, and an object system.

Bug Fix

BZ#648498

Previously, snapshots from the Network File System (NFS) mounted home directories located on Network Appliance (NetApp) filers were treated as real mounts and were displayed on the desktop. Due to this behavior, users could not hide or unmount these items. By default, the GNOME desktop treated all mounts under user home directories as custom and put their icons on the desktop. This update follows common practice and hides mounts with path elements that start with a dot.

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

1.75. glibc

1.75.1. RHBA-2011:0584 — glibc bug fix and enhancement update

Updated glibc packages that fix numerous bugs and add various enhancements 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 Fixes

BZ#646954

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.

BZ#642584

On 64-bit x86 systems with support for AVX vector registers, an insufficient alignment of the thread descriptor could cause an application to crash during symbol resolution. With this update, the "TCB_ALIGNMENT" value has been increased to 32 bytes, and applications no longer crash.

BZ#641128

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#656530

The long double square root function, **sqrtl**, sometimes returned an incorrect result if the relative magnitude difference between the high and low halves of the long double exceeded a certain number. This occurred because one of the variables used in the calculation was an unsigned integer. The integer is now signed and the function works correctly.

BZ#623187

The **futex(FUTEX_WAKE_OP)** method did not default to **futex(FUTEX_WAKE)** when **FUTEX_WAKE_OP** was not supported by the kernel. This resulted in the method always failing on these systems. The code change in **glibc pthread_cond_signal()** that caused this issue has now been corrected.

BZ#661982

The memmove, wmemmove and wmemset operations contained incorrect "__restrict" qualifiers, even though their arguments could overlap. This issue has now been corrected.

BZ#656014

The name service cache daemon (nscd) cached the results of lookups for DNS records even when the DNS records had a time-to-live of 0. nscd now respects DNS time-to-live values, and does not cache the results in this situation.

BZ#653905

Attempting to build the glibc RPM failed when **%_enable_debug_packages** was either not set, or set to 0. This has been corrected so that debug packages need not be set or enabled in order to build the glibc RPM.

BZ#652661

An uninitialized variable prevented glibc from compiling with the G++ compiler when "sys/timex.h" was included. This has been corrected.

BZ#647448

strchr did not handle its second parameter correctly when %rdi was aligned to a 16-byte boundary and glibc was enabled for multiple architectures on AMD64 or Intel 64 systems with CPUs that supported Supplemental Streaming SIMD Extension (SSE) 4.2. The method would therefore output incorrect results. This has been corrected, and **strchr** now gives the expected output.

BZ#615701

glibc did not load nosegneg libraries in a 32-bit Xen domain U environment when **hwcap 1 nosegneg** was set in **/etc/ld.so.conf.d/nosegneg.conf**, causing the incorrect library to be used. This has been corrected so that the nosegneg libraries are loaded.

BZ#692177

Previously, the **sysconf(_SC_*CACHE)** method returned **0** for all caches on systems with Intel Xeon processors. This occurred because glibc used cpuid leaf 2 rather than cpuid leaf 4. This update uses cpuid leaf 4 where possible, resolving this issue.

BZ#689471

The **strncmp** method failed with a segmentation fault when used with Supplemental Streaming SIMD Extension 4 (SSE4). Several checks have been implemented to prevent this.

Enhancements

BZ#601686

Several aspects of glibc code have been optimized for Supplemental Streaming SIMD Extension (SSE), including **memcpy()**, **strcasecmp()**, **strnlen()**, **strcasestr()** and **strncasestr()**.

BZ#615090

Details about the MALLOC_PERTURB_ (M_PERTURB) operation, which can be used to debug the use of uninitialized or freed heap memory, have been added to the documentation.

BZ#676076

Support for forthcoming AMD processors has been added to glibc's **memset** operation.

All users of glibc are advised to upgrade to these updated packages, which resolve these issues.

1.75.2. RHBA-2011:1179 — glibc bug fix update

Updated glibc packages that resolve several issues are now available for Red Hat Enterprise Linux 6.

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#712125

Under certain circumstances, a threaded process could have been granted incomplete group membership of the user which was running the process. This was caused by glibc using its default method for group membership determination, which led to a situation in which multiple threads interfered with each other while attempting to retrieve 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#712407

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 the 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#712411

Prior to this update, the Name Service Caching Daemon (nscd) did not clear the host cache effectively when repopulating its values. The code has been modified to schedule nscd cache pruning more accurately.

BZ#715387

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 resolve these issues.

1.76. gnome-panel

1.76.1. RHBA-2011:0710 — gnome-panel bug fix and enhancement update

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

The GNOME panel provides the window list, workspace switcher, menus, and other features for the GNOME desktop. libwnck allows applications to monitor information about open windows, workspaces, their names/icons, and so forth.

Bug Fixes

BZ#607665

Previously, when a user connected two monitors to a computer and set the GNOME Panel to show hide buttons, the panel did not hide but moved to the adjacent monitor instead. This bug has been fixed, moving the panel to the adjacent monitor no longer takes place.

BZ#633853

Previously, there was the untranslated text label "Top Panel" in the GNOME Panel's "Add to Panel" dialog. The problem applied to all non-English locales. The problem has been resolved so that the untranslated text label does not appear anymore in the "Add to Panel" dialog.

BZ#633870

Previously, there was a conflicting accelerator key in the GNOME Panel's Date/Time context menu under the kn_IN locale. The fix for this bug has been provided so that there is no more a conflicting accelerator key in the Date/Time context menu.

Enhancements

BZ#509061, BZ#673231

When windows were grouped by the GNOME Panel in the taskbar, they were grouped in an alphabetical order. Such behavior presented a problem when window title changed. This release introduces an option to disable grouping window alphabetically. The fix to enable the option has been applied both in the gnome-panel and the libwnck package.

BZ#585312

Previously, when an external monitor was connected to a computer, a user was able to move a panel between monitors by pressing the Alt key and dragging a blank area of the panel. This update

introduces an enhancement in that the user can now change the settings with regard to moving the panel between monitors in the GNOME Panel "Properties" dialog.

All users requiring gnome-panel and libwnck should upgrade to these updated packages, which resolve these issues and add these enhancements.

1.77. gnome-power-manager

1.77.1. RHBA-2011:0722 — gnome-power-manager bug fix update

Updated gnome-power-manager packages that fix several bugs are now available.

GNOME Power Manager uses the information and facilities provided by HAL to display icons and handle user callbacks in an interactive GNOME session.

Bug Fixes

BZ#581525

Previously, the Help page for GNOME Power Manager was not displayed when users pressed F1 or selected Help from the menu bar. This has been corrected and the Help page now appears as expected.

BZ#623674

The "do nothing" option, which allowed users to work on external monitors even when their laptop lid was closed, was removed. This prevented users from using external monitors while their laptop was closed. The "do nothing" option has been reinstated to allow this.

BZ#624422

A bug in the docbook2man tool caused the GNOME Power Manager man page (man gnome-power-manager) to appear incorrectly. The man page has been manually corrected while this bug is in effect.

BZ#640296

When an attempt to hibernate failed, an alert was displayed prompting users to check a help file. However, there was no link to the help file, which caused confusion. The alert no longer refers to the help file.

All users of GNOME Power Manager are advised to upgrade to these updated packages, which resolve these issues.

1.78. gnome-terminal

1.78.1. RHBA-2011:0700 — gnome-terminal bug fix update

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

Gnome-terminal is a terminal emulator for GNOME. It supports translucent backgrounds, opening multiple terminals in a single window (tabs) and clickable URLs.

Bug Fix

BZ#669113

Changes made to check boxes in the search dialog were not reflected in the terminal engine (vte). This led to confusion and wrong functionality. Problem has been fixed and users should get expected behaviour.

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

1.79. gpxe

1.79.1. RHBA-2011:0694 — gpxe bug fix update

Updated gpxe packages that fix two bugs 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 Fixes

BZ#661840

Devices that did not allow interrupts or required polling were not supported by gPXE UNDI code. This meant that booting did not work when using gPXE images on bare metal with some NICs, such as Emulex 10g. This patch allows the gPXE UNDI code to use polling for underlying devices that do not support interrupts. As a result it is now possible to use gPXE images to boot bare metal hosts using UNDI where it was not possible in some cases.

BZ#672529

Virtual Machines (VM) with virtIO NIC could not access the PXE server, reaching a time out. This was because even though the VM could get an IP address from the DHCP server, it could not reach its own default gateway. The ARP requests that the VM sends were too large and thus not valid, so the default gateway did not answer those ARP requests. A patch has been added that sets the size of the transmitted Ethernet frame to header + data length, allowing the VM to boot via PXE.

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

1.80. grub

1.80.1. RHEA-2011:0633 — grub enhancement update

An updated grub package that adds two enhancements is now available for Red Hat Enterprise Linux 6.

The GRUB utility is responsible for booting the operating system kernel.

Enhancements

BZ#553741

Prior to this update, GRUB only supported the MD5 password encryption. This update introduces support for the SHA-2 cryptographic algorithms, allowing users to encrypt passwords using SHA-256 and SHA-512 hash functions as well.

BZ#654869

GRUB has been updated to allow booting from disk drives with 4KB sector size on UEFI systems.

All users of grub are advised to upgrade to this updated package, which adds these enhancements.

1.80.2. RHBA-2011:1476 — grub bug fix update

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

The GRUB utility is responsible for booting the operating system kernel.

Bug Fix

BZ#742976

An attempt to install GRUB on a CCISS device may have caused the grub-install utility to report the following error:

```
expr: non-numeric argument
```

When this happened, grub-install failed to install GRUB on this device, but incorrectly reported success and returned a zero exit status. This update applies a patch that ensures that GRUB can now be successfully installed on such devices.

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

1.81. gtk2

1.81.1. RHBA-2011:0693 — gtk2 bug fix update

Updated gtk2 packages that fix two file chooser bugs and two translation problems are now available for Red Hat Enterprise Linux 6.

GTK+ is a multi-platform toolkit for creating graphical user interfaces.

Bug Fixes

BZ#647922

In the "Open Files" dialog box, the file selected by default failed to be opened upon hitting Enter if the "Location" field was displayed. Users had to select the file manually to actually open it. This update provides a fix to address this issue and the file selected by default now opens correctly.

BZ#647923

The "Open Files" dialog box failed to show contents of the directory selected by default upon hitting Enter if the "Location" field was displayed. Users had to select the directory manually to actually show its contents. This update provides a fix for this issue and the directory selected by default now shows its contents correctly.

BZ#625440

There was a typo in the Marathi (mr_IN) and Telugu (te_IN) translations. Erroneous "calender:MY" string was part of those translations. This update provides corrected translations.

BZ#636476

There was an inconsistency in the Guarati (gu_IN) translation. In ibus's Language Selection Tab, titles for "Up" and "Down" buttons and help labels at the bottom of the dialog box did not match. This update provides an updated translation.

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

1.82. gvfs

1.82.1. RHBA-2011:0536 — gvfs bug fix and enhancement update

Updated gvfs packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

GVFS is the GNOME desktop's virtual file system layer, which allows users to easily access local and remote data, including via the FTP, SFTP, WebDAV, CIFS and SMB protocols, among others. GVFS integrates with the GIO (GNOME I/O) abstraction layer.

Bug Fixes

BZ#616145

A flaw in the GVFS client code prevented D-Bus communications from being parsed correctly. Due to this problem, Nautilus became unresponsive when the user attempted to view Trash if a folder with an attached emblem was moved to Trash. This update corrects an error in the enumeration code which resolves this problem. Now, Nautilus no longer becomes unresponsive in such cases.

BZ#616838

Previously, an unused file descriptor was not closed after a fork. Due to this behavior, SELinux prevented /usr/bin/ssh access to the leaked /dev/ptmx file descriptor. This update closes the leaked file descriptor. Now, SELinux alerts no longer appear.

BZ#636540

Previously, the gnome-disk-utility packages did not reflect current version requirements. Due to this lack, potential problems could arise with custom compiled packages. This update requires the correct version of gnome-disk-utility packages.

BZ#645630

Previously, the gvfsd-archive command was unexpectedly aborted when the user attempted to mount an archive file a second time. This update changes the way the gvfsd-archive backend is finalized. Now, gvfsd-archive no longer aborts when the same archive files are mounted for the second time.

BZ#667367

Running the "gvfs-mkdir --help" command caused "--delete-files" to appear instead of "--create-directories". This update fixes the gvfs-mkdir command's help output so that the correct options are displayed.

Enhancement

BZ#624795

Previously, snapshots from the Network File System (NFS) mounted home directories located on Network Appliance (NetApp) filers were treated as real mounts and were displayed on the desktop. This behavior could cause confusion. This update checks and hides mounts with a path element

starting with a dot. With this update, these mounts are hidden. Now, snapshot directories are no longer shown in the GUI. To apply this enhancement, the updated glib2 packages must be installed as well.

Users of GVFS are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

1.83. hal

1.83.1. RHBA-2011:0724 — hal bug fix update

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

HAL is daemon for collecting and maintaining information from several sources about the hardware on a system.

Bug Fixes

BZ#576048

Previously, the init script for hald did not parse a config file in /etc/sysconfig. This meant that the only way to pass extra parameters to the hald was to start them manually without the init script, or to modify the line that launches hald in the init script itself. This update changes the startup script to parse a config file in /etc/sysconfig for extra configuration parameters.

BZ#676618

When checking hal-device on a device that did not exist, an error in dbus/hal communication was displayed. In this update, hal no longer tries to close shared DBus connections, and therefore avoids printing a warning.

Users are advised to upgrade to this updated hal package, which resolves these issues.

1.84. hivex

1.84.1. RHBA-2011:0588 — hivex bug fix and enhancement update

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

Hive files are undocumented binary blobs that Windows uses to store the Windows Registry on the disk. Hivex is a library that can read and write to these files.

Bug Fix

BZ#657017

Due to a problem with the Perl hivex bindings in the spec file, rebuilding of source packages could have failed if compiled from the source RPM. With this update, the issue no longer occurs.

Enhancement

BZ#642631

The hivex package was updated to the upstream version 1.2.3. This enhancement provides several stability improvements.

All hivex users are advised to upgrade to these updated hivex packages, which resolve this issue and add this enhancement.

1.85. hplip

1.85.1. RHBA-2011:0574 — hplip bug fix update

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

The hplip packages contain the Hewlett-Packard Linux Imaging and Printing Project (HPLIP) which provides drivers for Hewlett-Packard printers and multi-function peripherals.

Bug Fixes

BZ#608003

Previously, certain Python scripts used the interpreter line "#!/usr/bin/env python". Due to this issue, these scripts used an incorrect version during the execution. With this update, the interpreter line is changed and uses the path /usr/bin/python.

BZ#613707

Previously, the license text was missing. This update adds the license text to the hplip-common sub-package.

BZ#616569

Previously, the hp-toolbox utility failed to add new printers due to incorrect handling of CUPS authentication in the cupsext Python extension. This update corrects the handling. Now, new printers can be added successfully.

BZ#633899

Previously, the CUPS Web Interface button, displayed in hp-toolbox when no connected devices were shown, led to an incorrect URL. This update corrects this URL so that there is no error message shown.

BZ#652255

This update upgrades HPLIP to the current version to allow support for a wider range of HP printers.

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

1.86. httpd

1.86.1. RHSA-2011:1245 — Important: httpd security update

Updated httpd 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 Apache HTTP Server is a popular web server.

Security Fix

CVE-2011-3192

A flaw was found in the way the Apache HTTP Server handled Range HTTP headers. A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially-crafted Range header.

All httpd users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

1.86.2. RHSA-2011:1391 — Moderate: httpd security and bug fix update

Updated httpd 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Apache HTTP Server is a popular web server.

Security Fixes

CVE-2011-3368

It was discovered that the Apache HTTP Server did not properly validate the request URI for proxied requests. In certain configurations, if a reverse proxy used the ProxyPassMatch directive, or if it used the RewriteRule directive with the proxy flag, a remote attacker could make the proxy connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to the attacker.

CVE-2011-3348

It was discovered that mod_proxy_ajp incorrectly returned an "Internal Server Error" response when processing certain malformed HTTP requests, which caused the back-end server to be marked as failed in configurations where mod_proxy was used in load balancer mode. A remote attacker could cause mod_proxy to not send requests to back-end AJP (Apache JServ Protocol) servers for the retry timeout period or until all back-end servers were marked as failed.

Red Hat would like to thank Context Information Security for reporting the CVE-2011-3368 issue.

Bug Fix

BZ#736592

The fix for CVE-2011-3192 provided by the RHSA-2011:1245 update introduced regressions in the way httpd handled certain Range HTTP header values. This update corrects those regressions.

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

1.86.3. RHBA-2011:0706 — httpd bug fix update

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

The Apache HTTP Server is a popular web server.

Bug Fixes

BZ#631849

Due to a bug in the filter initialization process, filters configured using the mod_filter module were not handled correctly if a "sub-request" took place. For example, using the "FilterChain" directive to configure the "DEFLATE" compression filter with a Server-Side-Include page could result in pages which were only partially compressed. With this update, filters used with mod_filter operate correctly.

BZ#657480

If arguments passed to the ab benchmarking program triggered a memory allocation failure, ab could terminate unexpectedly with a segmentation fault. With this update, the memory allocation failure is now trapped earlier, and the program exits gracefully with an error message. (BZ#645846) * When executing the "service httpd stop" command, a 10-seconds timeout is used before terminating the httpd parent process in case of error. If this timeout was insufficient, resources did not allow the parent process to terminate cleanly and could be leaked. This update introduces the "STOP_TIMEOUT" environment variable, which can be used in the /etc/sysconfig/httpd configuration file to change the timeout. This can be used to allow a longer delay and fix resource leaks if the httpd parent is slow to terminate.

BZ#676635

When configuring the httpd service, using a mod_ldap directive in the "VirtualHost" container caused the HTTP server to stop caching requests to a directory server. This update applies a patch that corrects this error, and the use of mod_ldap directives in the "VirtualHost" context no longer prevents the httpd service from caching LDAP requests.

BZ#676831

Prior to this update, an attempt to use configuration with multiple virtual hosts sharing the same ID and private key file could prevent the httpd service from starting with an error message written to the error_log file. With this update, the underlying source code has been modified to address this issue, and the httpd service now starts as expected.

BZ#679476

When using the prefork Multi-Processing Module (MPM), children processes with persistent connections (that is, with the "KeepAlive" directive set to "On") kept processing new requests even when a graceful restart had been issued. This update applies a patch that corrects this error, and children processes with the persistent connections no longer process new requests when a graceful restart is requested.

BZ#684144

Previously, an attempt to start the httpd service with the mod_ssl module in FIPS mode failed. With this update, an upstream patch has been applied to implement support for the FIPS mode in the mod_ssl module, and httpd no longer fails to start.

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

1.87. hwdata

1.87.1. RHEA-2011:0701 — hwdata enhancement update

An updated hwdata package that adds various enhancements is now available for Red Hat Enterprise Linux 6.1.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

Enhancements

BZ#662673

The pci.ids database has been updated to include the information about the MegaRAID SAS Thunderbolt device.

BZ#633837

The pci.ids database has been updated to include the information about the Matrox IMMv2 management controller and integrated MatroxG200eR video controller.

Users of hwdata are advised to upgrade to this updated package, which adds these enhancements.

1.88. ibus

1.88.1. RHBA-2011:0518 — ibus bug fix update

Updated ibus packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

The IBus (Intelligent Input Bus for Linux OS) package is an input method platform.

Bug Fixes

BZ#651915

ibus-x11 displayed at the incorrect window position and did not follow xterm for X11 applications in big endian 64-bit machines such as ppc64 and s390x. This was caused by the call_data->ic_attr[i].value being able to support only CARD32 data (32-bit) while the problematic machines were 64-bit machines. The code was changed to support 64-bit machines, thus ibus now works as expected.

BZ#633330

ibus displayed incorrect text for the "up" and "down" buttons for the Kannada translation. The translated text was corrected, thus now the buttons display the correct translated text.

BZ#635541

ibus displayed inconsistent translations on "up" and "down" buttons compared to text at the bottom of the window referring to "up" and "down" buttons for the Gujarati translation. Translation was amended for consistency and the button text and descriptive text at the bottom of the window are now the same.

Users of ppc64, s390x machines, Gujarati, and Kannada, are advised to upgrade to these updated packages, which resolve these issues.

1.89. ibus-chewing

1.89.1. RHBA-2011:0737 — ibus-chewing bug fix update

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

IBus-chewing is an IBus front-end of Chewing, an intelligent Chinese input method for Zhuyin (BoPoMoFo) users.

Bug Fix

BZ#627794

Previously, the IBus-chewing did not specify the rank parameter for the zh-TW locale in the input engine description file. This caused the IBus tool not to provide any default input method engine for the locale. This update adds the input method engines to the chewing.xml file and ibus-chewing is selected as the default input method for zh_TW users.

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

1.90. ibus-hangul

1.90.1. RHBA-2011:0538 — ibus-hangul bug fix update

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

The ibus-hangul package is a Korean language input engine platform for the IBus input method (IM).

Bug Fix

BZ#610075

Previously, preedit was not restored when the candidate window was restored while focusing in. Due to this behavior, the candidate window remained open after focus changes. This update resolves this issue with a change in the code. Now, the candidate window is hidden as expected.

Users who require Korean language input are advised to upgrade to this updated package, which fixes this bug.

1.91. ibus-m17n

1.91.1. RHBA-2011:0539 — ibus-m17n bug fix update

An updated ibus-m17n package that resolves several bugs is now available.

The ibus-m17n is a multilingual input engine for the IBus input method platform.

Bug Fixes

BZ#641243

When a new user and language were selected during login, ibus-m17n did not load all input methods provided for that language; only one input method was loaded and marked for use as the default input method. The user had to manually search for and add any other input methods that they wanted to use. All input methods for a given language are now loaded upon login, and can be accessed from the ibus-m17n Preferences tab.

BZ#652201

ibus-m17n did not recognize the AltGr (ISO Level 3 Shift) key as a virtual modifier key, making it impossible to input the Rupee Symbol (U+20B9) with an Indic Keyboard. The AltGr key is now recognized by ibus-m17n.

All users of ibus-m17n are advised to upgrade to this updated package, which resolves these issues.

1.92. ibutils

1.92.1. RHBA-2011:0814 — ibutils bug fix update

Updated ibutils packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

The ibutils package provides InfiniBand network and path diagnostics.

Bug Fix

BZ#695204

Previous releases of the ibutils package were not built for the PowerPC 64-bit architecture. This has been fixed and the ibutils package is now built for the PowerPC 64-bit architecture as well.

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

1.93. icedtea-web

1.93.1. RHSA-2011:1100 — Moderate: icedtea-web security update

Updated icedtea-web packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

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

The IcedTea-Web project provides a Java web browser plug-in and an implementation of Java Web Start, which is based on the Netx project. It also contains a configuration tool for managing deployment settings for the plug-in and Web Start implementations.

Security Fixes

CVE-2011-2514

A flaw was discovered in the JNLP (Java Network Launching Protocol) implementation in IcedTea-Web. An unsigned Java Web Start application could use this flaw to manipulate the content of a Security Warning dialog box, to trick a user into granting the application unintended access permissions to local files.

CVE-2011-2513

An information disclosure flaw was discovered in the JNLP implementation in IcedTea-Web. An unsigned Java Web Start application or Java applet could use this flaw to determine the path to the cache directory used to store downloaded Java class and archive files, and therefore determine the user's login name.

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

1.93.2. RHSA-2011:1441 — Moderate: icedtea-web security update

Updated icedtea-web 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 IcedTea-Web project provides a Java web browser plug-in and an implementation of Java Web Start, which is based on the Netx project. It also contains a configuration tool for managing deployment settings for the plug-in and Web Start implementations.

Security Fix

CVE-2011-3377

A flaw was found in the same-origin policy implementation in the IcedTea-Web browser plug-in. A malicious Java applet could use this flaw to open network connections to hosts other than the originating host, violating the same-origin policy.

All IcedTea-Web users should upgrade to these updated packages, which upgrade IcedTea-Web to version 1.0.6 to correct this issue. Web browsers using the IcedTea-Web browser plug-in must be restarted for this update to take effect.

1.94. im-chooser

1.94.1. RHBA-2011:0666 — im-chooser bug fix update

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

im-chooser is a GUI configuration tool to choose the Input Method to be used or disable Input Method usage on the desktop.

Bug Fix

BZ#634146

The im-chooser window was not re-sizable. This caused the title bar text to run into the right-hand close box in some locales. With this update, the im-chooser window is now re-sizable, ensuring the title bar text displays properly no matter the current locale.

All im-chooser users are advised to upgrade to this updated package, which resolves this issue.

1.95. imsettings

1.95.1. RHBA-2011:0521 — imsettings bug fix update

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

The imsettings packages provide a library and command line tools to configure and control input-methods settings. Users normally access it through the "im-chooser" GUI tool.

Bug Fix

BZ#616061

It was not possible to turn off the GTK XIM input-method module from imsettings. As a consequence, users were unable to enter Unicode characters using the Ctrl+Shift+U shortcut. With this update, the default GTK input-method is restored to gtk-im-context-simple, which allows Unicode input with the shortcut. Now only desktop locales that normally need X locale compose default to using the GTK XIM input-method module.

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

1.96. initscripts

1.96.1. RHBA-2011:0647 — initscripts bug fix and enhancement update

An enhanced initscripts package that fixes various bugs and provides an enhancement 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 Fixes

BZ#558575

Previously, initscripts used quoted strings as values following the **=~** operators and the strings were thus matched as literal strings. However, they should be matched as regular expressions. With this update, the quotes were dropped and the strings are matched as regular expressions as expected.

BZ#598850

Previously, some systems failed to access the harware clock on system shutdown. This happened because the shutdown script ran the **hwclock** tool, which attempted to access the **/dev/rtc** device even if it did not exist. With this update, initscripts verifies if the **/dev/rtc** device exists before attempting to run the **hwclock** tool.

BZ#612934

The **ifdown** command could have failed to stop an NIC (Network Interface Controller) with a warning that the connection was unknown. This happened because, in some cases, the function, which verifies whether the NIC is managed by NetworkManager, returned an incorrect result. With this update, the function returns the correct result and the **ifdown** command stops the NIC correctly.

BZ#620461

Previously, if there was a bind mount for the **/** directory, the system could have failed to remount the root directory as a read-only file system on shutdown. This occurred because the script attempted to remount the defined bind mount instead of the root directory. With this update, the root directory is remounted successfully.

BZ#629257

Previously, a conflict between the sulogin tool and the login shell could have prevented the user from

entering the root password in single-user mode. This occurred when switching from runlevel 3 because the login shell was not terminated and attempted to accept the input for the sulogin tool. With this update, the **tty.conf** and **serial.conf** files have been modified to have the login shell stopped when changing to runlevels S and the problem no longer occurs.

BZ#632584

On interactive startup, in some locals, the shortcut of the **Continue** key in the respective language did not work. This occurred due to an error in the local po files. With this update, the po files have been updated and the shortcuts work as expected.

BZ#633984

Previously, the network service did not support configurations with multiple IP addresses with the new syntax (IPADDRESSn/PREFIXn). This caused conflicts between network configurations set with the network service and network configurations set with the **NetworkManager** tool. With this update, the network service supports the configurations with multiple IP addresses with the new syntax and the conflicts no longer occur.

BZ#634996

Previously, the **tty.conf** file contained a comment with a typographical mistake (**"sepcified"**). With this update, the word is spelled correctly (**"specified"**).

BZ#635360

Previously, the system was not able to create a logical network with the VLAN (virtual local area network) tag value **0**. With this update, this tag value is allowed.

BZ#637058

Previously, the **/etc/sysconfig/clock** file did not document where the user can configure whether the **hwclock** tool should be using the local time or UTC (Coordinated Universal Time). This update adds comments documenting the setting location into the **sysconfig.txt** file.

BZ#645861

Previously, the **/etc/ppp/ipv6-up** and **/etc/ppp/ip-up.ipv6to4** scripts used the incorrect alias **ipv6_exec_ip** and failed to bring up the routes. This update modifies the scripts so that they uses the **ip** command and the routes are now brought up as expected.

BZ#648966

For IPoIB (IP over InfiniBand) child interfaces, the value of the **DEVICETYPE** variable was calculated incorrectly. This happened because the calculation preserved the period (**.**) sign in the device name. This could have caused failure of the **ifup-ib** and **ifdown-ib** scripts. With this update, **DEVICETYPE** is resolved correctly.

BZ#654101

On shutdown, the system tried to deactivate the sit IPv6 over IPv4 tunnel device even though it was not active. With this update, the system verifies if the device is active before attempting to shut it down.

BZ#658138

Previously, the **kexec-disable** script was run when switching to runlevel 1. Because the **kdump** service is disabled in runlevel 1, the script freed the memory reserved for **kdump**. After the user

changed from runlevel 1 to runlevel 3, which has **kdump** enabled, the system had set reserved memory size to 0 and **kdump** failed to start up. With this update, the kexec-disable job is no longer run in runlevel 1.

BZ#660036

Previously, all architectures used identical ***shmmax*** (maximum size of a shared memory segment) and ***shmall*** (maximum size of the total shared memory) values. However, the values vary depending on the system architecture. This update provides the settings of these values for various architectures.

BZ#664051

Previously, various errors occurred when some devices were inserted (for example, PCI network card). This happened because the **biodevname** tool assigned them interface names containing hash (#) signs, which were forbidden in such names. With this update, interface names can contain hash (#) signs and the problem no longer occurs.

BZ#667211

Previously, initscripts did not distinguish between the period (`.`) signs used by the **sysctl** device, which were delimiting the paths, and the period (`.`) signs used by VLANs, which were delimiting IDs. This caused that all sysctl calls to the VLAN interfaces failed. With this update, when calling a sysctl device, initscripts substitutes the periods in its name with forward slash (`/`) signs and the sysctl calls to a VLAN interface succeed.

BZ#669110

Previously, a slave network interface of a bonded interface failed to start if it defined the setting ***MASTER*** in double quotes (for example, as **"bond0"**). With this update, the respective scripts have been adapted to parse the value definition correctly even if double-quoted.

BZ#670154

The **ifdown** command could have failed to stop a bridge device with a warning that the connection was unknown. This happened because the function, which verified whether the device is managed by **NetworkManager**, returned an incorrect result. With this update, the function returns a correct result and the **ifdown** command stops the bridge device correctly.

BZ#674397

Section 8 of the sys-unconfig manual page contained various typographical mistakes. With this update, the man page is updated and the mistakes are corrected.

BZ#676708

Previously, a name of a VLAN interface had to start with the **eth** prefix followed by digits. If the user provided a name, which did not follow these requirements, the interface could not be started or stopped. With this update, the user can provide a custom name and the interface can be operated correctly.

BZ#696110

Previously, the **netfs** startup script attempted to run the **mdadm** tool always when the **/etc/mdadm.conf** file existed and could have failed if mdadm was not installed. With this update, the script first verifies if the mdadm tool is installed and only then runs its binary.

BZ#682879

The system could have failed to unmount the NFS (Network File System) shares on shutdown. This occurred because the system failed to unmount the NFS shares if they were in use. With this update, the unmouting of NFS shares on shutdown has been updated and the NFS shares are unmounted successfully even if in use.

Enhancement

BZ#633323

With this update, the IBM System z profile was updated to allow an optimized performance setting for System z.

All users are advised to upgrade to this updated package, which fixes these bugs and provides this enhancement.

1.97. iok

1.97.1. RHBA-2011:0555 — iok bug fix update

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

iok is an Indic on-screen virtual keyboard that supports the Assamese, Bengali, Gujarati, Hindi, Kannada, Marathi, Malayalam, Punjabi, Oriya, Sindhi, Tamil and Telugu languages. Currently, iok works with Inscript and xkb keymaps for Indian languages, and is able to parse and display non-Inscript keymaps as well.

Bug Fix

BZ#636756

The file that contains the Oriya translations for iok contained some entries with Latin text appended to the Oriya text. The Latin text caused the key size to increase, thus the keyboard became too large to fit in the display area. The Latin text has now been removed from the Oriya translation, causing the Oriya keyboard and keys size to conform to other languages.

Users are advised to upgrade to this updated iok package, which resolves this issue.

1.98. ipa

1.98.1. RHBA-2011:1314 — ipa bug fix update

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

Red Hat Enterprise Identity (IPA) is a centralized authentication, identity management, and authorization solution for both traditional and cloud-based enterprise environments. It integrates components of the Red Hat Directory Server, MIT Kerberos, Red Hat Certificate System, NTP, and DNS.

Bug Fix

BZ#729805

Prior to this update, GSSAPI credential delegation was disabled in the curl utility due to a security issue. As a result, applications that rely on delegation did not work properly. This update utilizes a new constructor argument in the xmlrpc-c client API to set the new

CURLOPT_GSSAPI_DELEGATION curl option. This option enables the credential delegation, thus fixing this bug.

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

1.98.2. RHBA-2011:0865 — ipa bug fix update

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

Red Hat Enterprise Identity (IPA) is a centralized authentication, identity management and authorization solution for both traditional and cloud based enterprise environments. It integrates components of the Red Hat Directory Server, MIT Kerberos, Red Hat Certificate System, NTP and DNS. It provides web browser and command-line interfaces. Its administration tools allow an administrator to quickly install, set up, and administer a group of IPA servers to meet the authentication and identity management requirements of the large scale Linux and Unix deployments.

Bug Fixes

BZ#709329

When an IPA server was installed and then a replica package for a replica server was generated, the installation of the replica server failed. With this update, the installation process waits for the 389DS (389 Directory Server) tasks to complete before restarting the server, fixing this bug.

BZ#709330

Previously, the ipa service was not enabled via the chkconfig tool during the installation of a replica server. Subsequently, when the replica server was restarted, the ipa service was not started. With this update, replica servers are properly configured to start on boot.

BZ#709331

After a replica server was installed, the Managed Entries were not properly configured on replica servers. Subsequently, users had to manually add the configuration using the ldapmodify tool after the replica installation, and then restart the services with the "ipactl restart" command. This bug has been fixed and the configuration is now automatically added as expected.

BZ#709332

When a new reverse zone was created via the ipa-replica-prepare script, the wrong DNS entry was updated, which eventually caused an installation of a replica server to fail. This bug has been fixed and when the named service is restarted after a replica package has been created, the correct DNS entries are now set up for an installation of a replica server.

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

1.99. ipmitool

1.99.1. RHEA-2011:0775 — ipmitool enhancement update

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

The ipmitool package contains a command line utility for interfacing with devices that support the Intelligent Platform Management Interface specification (IPMI). IPMI is an open standard for machine health, inventory, and remote power control.

Enhancements

BZ#631649

The update adds the "delloem" command extensions for Dell OEM hardware, which provide support for Peripheral Component Interconnect Express (PCIe) solutions, LCD setting on panel, NIC setting, and power monitoring. This update also provides manual pages for the "delloem" command extensions.

BZ#663793

This update integrates the Linux Multiple Device (MD) driver with ipmitool to indicate SES (SCSI enclosure services) status and drive activities for PCIe SSD based solutions.

Users of ipmitool are advised to upgrade to this updated package, which adds these enhancements.

1.100. iproute

1.100.1. RHBA-2011:0757 — iproute bug fix and enhancement update

Updated iproute packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The iproute packages contain networking utilities designed to use the advanced networking capabilities of the Linux kernel.

Bug Fix

BZ#636943

If the "ip" command was used to create a veth device pair, and the "peer" parameter was specified but the "name" parameter was not used, a segmentation fault occurred. The "name" parameter was an unnecessary requirement for this operation. The need for this parameter has been removed and the command now works as expected.

BZ#641918

The ss man page contained a reference to a nonexistent file. This reference has been updated with the correct file location.

BZ#678986

Previously, attempting to flush a secondary device with "ip secondary" would fail. This issue has now been corrected and secondary devices are flushed as expected.

Enhancement

BZ#670295

Support for adding, deleting, and modifying security contexts or security labels in ipsec policies has been added to the "ip xfrm" command.

All users of iproute are advised to upgrade to these updated packages, which correct these issues and add this enhancement.

1.101. iprutils

1.101.1. RHEA-2011:0643 — iprutils enhancement update

An updated iprutils package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The iprutils package provides utilities to manage and configure SCSI devices that are supported by the "ipr" SCSI storage device driver.

Enhancement

BZ#633328

The iprutils package has been updated to provide support for the 6Gb SAS RAID storage controller on 64-bit IBM POWER7.

All users of iprutils are advised to upgrade to this updated package, which adds this enhancement.

1.101.2. RHBA-2011:1474 — iprutils bug fix update

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

The iprutils package provides utilities to manage and configure SCSI devices that are supported by the IBM Power RAID SCSI storage device driver.

Bug Fixes

BZ#747621

Due to an incorrectly placed call of the sysfs_close_bus() structure in the iprlib code, some of the iprutils programs could terminate unexpectedly with a segmentation fault during their initialization. This problem has been corrected, and iprutils programs no longer crash.

BZ#747621

The find_multipath_vset routine used the ARRAY_SIZE() macro to calculate the length of the SCSI device serial number. Previously, the length was calculated incorrectly, which could have led to false positives when looking for the corresponding vset. As a consequence, attempting to delete arrays failed: the target and the second array were set to be read/write protected, writing to both arrays was not possible, and the system had to be rebooted. To fix the problem, the IPR_SERIAL_NUM_LEN macro is now used instead of ARRAY_SIZE.

BZ#747621

With the maximum number of devices attached to one of the new Silicon Integrated Systems (SiS) 64-bit adapters, the configuration data could have grown over the buffer size. With this update, the buffer size has been increased, which fixes the problem and ensures enough space for any possible future growth.

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

1.102. iptables

1.102.1. RHBA-2011:0557 — iptables bug fix and enhancement update

Updated iptables packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The iptables utility controls the network packet filtering code in the Linux kernel.

Bug Fixes

BZ#590186

Previously, ip6tables did not support Portable Transparent Proxy Solution (TPROXY). Due to this lack, the IPv6 transparent proxy support was missing and IPv6 transparency was not available. This update adds this option.

BZ#644273

Previously, the command "service iptables save" did not restore the context for the save file and the save backup file. It also used /tmp for the temporary file. Due to the wrong context of the save and save backup file, there could be an error the next time the save functionality is used. This update restores the context and also saves the temporary files correctly.

Enhancement

BZ#642393

Previously, iptables did not support auditing. Due to this issue, information for remote address/port, target address/port, protocol, and result (success/fail) could not be recorded as an audit event. This update adds the required audit support. This enhancement depends on the presence of auditing support in the kernel.

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

1.102.2. RHBA-2012:0336 — iptables bug fix update

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

The iptables utility controls the network packet filtering code in the Linux kernel.

Bug Fix

BZ#786871

The option parser of the iptables utility did not correctly handle the "-m mark" and "-m conmark" options in the same rule. Therefore, the iptables command failed when issued with both options. This update modifies behavior of the option parser so that iptables now works as expected with the "-m mark" and "-m conmark" options specified.

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

1.103. iputils

1.103.1. RHBA-2011:0546 — iputils bug fix update

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

The iputils package contains basic utilities for monitoring a network, including ping.

Bug Fixes

BZ#630022

The ping and ping6 commands were previously not compiled as position independent executables (PIE). In this update, they are now built as PIE executables.

BZ#671579

Previously, the tracepath6 program that is included in the iputils package failed to resolve a target when using the "-n" option and a hostname as the target. The fix for this problem has been provided so that tracepath6 now works as expected.

BZ#688332

Previously, when the rdisc utility that is included in the iputils package was run on a system with an interface having two IP addresses assigned to the interface, an error was issued and rdisc failed to start. The bug has been fixed and the rdisc start failure no longer occurs.

All iputils users should upgrade to this updated package, which resolves these issues.

1.104. irqbalance

1.104.1. RHBA-2011:0804 — irqbalance bug fix update

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

irqbalance is a daemon that evenly distributes IRQ load across multiple CPUs for enhanced performance.

Bug Fix

BZ#630023

irqbalance was not previously built with PIE and RELRO enabled, as they were in Red Hat Enterprise Linux 5. In this update, irqbalance is built as a PIE executable and is using RELRO protection.

Users of irqbalance are advised to upgrade to this updated package, which fixes this bug.

1.105. iscsi-initiator-utils

1.105.1. RHBA-2011:0733 — iscsi-initiator-utils bug fix and enhancement update

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

The iscsi package provides the server daemon for the Internet Small Computer System Interface (iSCSI) protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

Bug Fixes

BZ#691902

When performing SendTargets discovery, the "iface" NIC binding was ignored. Instead, iscsiadm used the network device determined by the "route" command. SendTargets discovery now occurs through the NIC specified in the "iface" binding information.

BZ#631821

If SendTargets discovery required multiple TEXT commands because of a long target list, iscsiadm did not set the Initiator Task Tag in compliance with RFC-3720 as published by the Internet Engineering Task Force. This issue has been fixed, and iscsiadm now sets the Initiator Task Tag correctly.

BZ#634021

Attempting to reboot or shut down a system with a running iSCSI daemon caused the system to stop responding because iSCSI sessions remained running. All iSCSI sessions now shut down correctly, so no issues are encountered on shut down or reboot.

BZ#689359

Previously, iSCSI did not work on the Broadcom NetXtreme II 1GbE Quad Port Copper Adapter (BCM57712) when connected to a Data Center Bridging-enabled (DCB-enabled) switch over VLAN. This occurred because VLAN tagging was set twice, once by uIP and once by the DCB firmware. This update corrects this issue with VLAN tagging.

BZ#640115

The ISCSI_ERR_INVALID_HOST error event was not being handled correctly, leaving iSCSI sessions in memory when the iSCSI driver was attempting to shut down. This resulted in the driver failing to respond during shutdown of sessions that used the Broadcom NetXtreme II Network Adapter driver.

BZ#593269

The iscsiadm and iscsid commands depended on files in /usr, but did not require that /usr was mounted when they were used. This resulted in failures without useful error messages when the user attempted to use these commands when /usr was not mounted. This issue has been corrected, and these failures no longer occur.

BZ#658428

Starting or stopping the iSCSI service while accessing the root partition directly through an iSCSI disk could cause iSCSI to become unresponsive and incorrect status information to be reported. Attempting to stop the iSCSI service in this circumstance now warns that iSCSI cannot be shut down while Root is on an iSCSI disk, and all statuses are reported correctly.

BZ#599539

The **brcm_iscsiuio** usage message displayed in response to the **brcm_iscsiuio --help** command contained two unsupported options: **--foreground** and **--pid**. The man page omitted five supported options: **--debug**, **--help**, **-h**, **-p** and **--version**. The unsupported options have been removed from the usage message, and all supported options have been added to the **brcm_iscsiuio** man page.

BZ#599542

The **iscsiadm** usage message displayed in response to the **iscsiadm --help** command omitted 24 supported options. Additionally, the **iscsiadm** man page omitted one supported option (**--host**) and contained one unsupported option (**--info**). These errors have now been corrected.

BZ#624437

iscsiadm did not accept host names or aliases as valid values for the **--portal** argument when in "node" mode. This resulted in failure, because iscsiadm expected the value returned during discovery

as the value for **`--portal`**. iscsiadm now attempts to match a host name to the IP address returned during discovery, so this issue no longer occurs.

BZ#688783

If debug message logging was disabled, the iSCSI daemon failed to set the socket priority according to the Data Center Bridging application priority setting, which resulted in packets being sent with the default priority incorrectly. Socket priority is now set based on the Data Center Bridging application priority setting in this situation.

Enhancements

BZ#640340

When iscsiadm failed or exited incorrectly, it did not output useful error codes. Meaningful error codes now exist for these situations, and are described further in the iscsiadm man page.

BZ#523492

Support for Data Center Bridging has been added to the iSCSI driver.

BZ#635899

brcm_iscsiuio provides the ARP and DHCP functionality to offload iSCSI functionality. Support has been added for IPv6, VLAN, and several new Broadcom network cards.

All users of iscsi-initiator-utils are advised to upgrade to these updated packages, which provide these bug fixes and add these enhancements.

1.106. iwl5000-firmware

1.106.1. RHBA-2011:0903 — iwl5000-firmware bug fix update

An updated iwl5000-firmware package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The iwl5000-firmware package provides the iwlagn wireless driver with the firmware it requires to function correctly with Intel Wireless WiFi Link 5000 series adapters.

This update upgrades the iwl5000 firmware to upstream version 8.83.5.1, which provides a number of bug fixes over the previous version. (BZ#709522)

Users of iwl5000-firmware are advised to upgrade to this updated package which fixes this bug.

1.107. iwl6000-firmware

1.107.1. RHBA-2011:0549 — iwl6000-firmware bug fix update

An updated iwl6000-firmware package is now available for Red Hat Enterprise Linux 6.

The iwl6000-firmware package provides the iwlagn wireless driver with the firmware it requires to function correctly with Intel Wireless WiFi Link 6000 series adapters.

This update upgrades the iwl6000 firmware to upstream version 9.221.4.1, which provides a number of bug fixes over the previous version. (BZ#568034)

Users of wireless devices which use iwl6000 firmware are advised to upgrade to this updated package.

1.108. iwl6050-firmware

1.108.1. RHBA-2011:0551 — iwl6050-firmware bug fix update

An updated iwl6050-firmware package is now available for Red Hat Enterprise Linux 6.

The iwl6050-firmware package provides the iwlagn wireless driver with the firmware it requires to function correctly with Intel Wireless WiFi Link 6050 series adapters.

This update upgrades the iwl6050 firmware to upstream version 41.28.5.1, which provides a number of bug fixes over the previous version. (BZ#663748)

Users of wireless devices which use iwl6050 firmware are advised to upgrade to this updated package.

1.109. java-1.5.0-ibm

1.109.1. RHSA-2011:1478 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

Security Fixes

CVE-2011-3545, **CVE-2011-3547**, **CVE-2011-3548**, **CVE-2011-3549**, **CVE-2011-3552**, **CVE-2011-3554**, **CVE-2011-3556**

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

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.5.0 SR13 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.109.2. RHSA-2011:1087 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

Security Fixes

CVE-2011-0802, **CVE-2011-0814**, **CVE-2011-0862**, **CVE-2011-0865**, **CVE-2011-0867**, **CVE-2011-0871**, **CVE-2011-0873**

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-FP5 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.110. java-1.6.0-ibm

1.110.1. RHSA-2011:0938 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

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

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

Security Fixes

CVE-2011-0802, **CVE-2011-0814**, **CVE-2011-0862**, **CVE-2011-0863**, **CVE-2011-0865**, **CVE-2011-0867**, **CVE-2011-0868**, **CVE-2011-0869**, **CVE-2011-0871**, **CVE-2011-0873**

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-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR9-FP2 Java release. All running instances of IBM Java must be restarted for the update to take effect.

1.111. java-1.6.0-openjdk

1.111.1. RHSA-2011:0856 — Critical: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 6.

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

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

Security Fixes

CVE-2011-0862

Integer overflow flaws were found in the way Java2D parsed JPEG images and user-supplied fonts. An attacker could use these flaws to execute arbitrary code with the privileges of the user running an untrusted applet or application.

CVE-2011-0871

It was found that the MediaTracker implementation created Component instances with unnecessary access privileges. A remote attacker could use this flaw to elevate their privileges by utilizing an untrusted applet or application that uses Swing.

CVE-2011-0864

A flaw was found in the HotSpot component in OpenJDK. Certain bytecode instructions confused the memory management within the Java Virtual Machine (JVM), resulting in an applet or application crashing.

CVE-2011-0867

An information leak flaw was found in the NetworkInterface class. An untrusted applet or application could use this flaw to access information about available network interfaces that should only be available to privileged code.

CVE-2011-0868

An incorrect float-to-long conversion, leading to an overflow, was found in the way certain objects (such as images and text) were transformed in Java2D. A remote attacker could use this flaw to crash an untrusted applet or application that uses Java2D.

CVE-2011-0869

It was found that untrusted applets and applications could misuse a SOAP connection to incorrectly set global HTTP proxy settings instead of setting them in a local scope. This flaw could be used to intercept HTTP requests.

CVE-2011-0865

A flaw was found in the way signed objects were deserialized. If trusted and untrusted code were running in the same Java Virtual Machine (JVM), and both were deserializing the same signed object, the untrusted code could modify said object by using this flaw to bypass the validation checks on signed objects.

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.

1.111.2. RHSA-2011:1380 — Critical: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

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

Security Fixes

CVE-2011-3556

A flaw was found in the Java RMI (Remote Method Invocation) registry implementation. A remote RMI client could use this flaw to execute arbitrary code on the RMI server running the registry.

CVE-2011-3557

A flaw was found in the Java RMI registry implementation. A remote RMI client could use this flaw to execute code on the RMI server with unrestricted privileges.

CVE-2011-3521

A flaw was found in the IIOP (Internet Inter-Orb Protocol) deserialization code. An untrusted Java application or applet running in a sandbox could use this flaw to bypass sandbox restrictions by deserializing specially-crafted input.

CVE-2011-3544

It was found that the Java ScriptingEngine did not properly restrict the privileges of sandboxed applications. An untrusted Java application or applet running in a sandbox could use this flaw to bypass sandbox restrictions.

CVE-2011-3548

A flaw was found in the AWTKeyStroke implementation. An untrusted Java application or applet running in a sandbox could use this flaw to bypass sandbox restrictions.

CVE-2011-3551

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the Java2D code used to perform transformations of graphic shapes and images. An untrusted Java application or applet running in a sandbox could use this flaw to bypass sandbox restrictions.

CVE-2011-3554

An insufficient error checking flaw was found in the unpacker for JAR files in pack200 format. A specially-crafted JAR file could use this flaw to crash the Java Virtual Machine (JVM) or, possibly, execute arbitrary code with JVM privileges.

CVE-2011-3560

It was found that HttpsURLConnection did not perform SecurityManager checks in the setSSLSocketFactory method. An untrusted Java application or applet running in a sandbox could use this flaw to bypass connection restrictions defined in the policy.

CVE-2011-3389

A flaw was found in the way the SSL 3 and TLS 1.0 protocols used block ciphers in cipher-block chaining (CBC) mode. An attacker able to perform a chosen plain text attack against a connection mixing trusted and untrusted data could use this flaw to recover portions of the trusted data sent over the connection.

CVE-2011-3547

Note: This update mitigates the CVE-2011-3389 issue by splitting the first application data record byte to a separate SSL/TLS protocol record. This mitigation may cause compatibility issues with some SSL/TLS implementations and can be disabled using the jsse.enableCBCProtection boolean

property. This can be done on the command line by appending the flag "-Djsse.enableCBCProtection=false" to the java command.

An information leak flaw was found in the InputStream.skip implementation. An untrusted Java application or applet could possibly use this flaw to obtain bytes skipped by other threads.

CVE-2011-3558

A flaw was found in the Java HotSpot virtual machine. An untrusted Java application or applet could use this flaw to disclose portions of the VM memory, or cause it to crash.

CVE-2011-3553

The Java API for XML Web Services (JAX-WS) implementation in OpenJDK was configured to include the stack trace in error messages sent to clients. A remote client could possibly use this flaw to obtain sensitive information.

CVE-2011-3552

It was found that Java applications running with SecurityManager restrictions were allowed to use too many UDP sockets by default. If multiple instances of a malicious application were started at the same time, they could exhaust all available UDP sockets on the system.

This erratum also upgrades the OpenJDK package to IcedTea6 1.9.10. Refer to the NEWS file for further information.

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.

1.111.3. RHBA-2011:0632 — java-1.6.0-openjdk bug fix and enhancement update

Updated java-1.6.0-openjdk packages that fix various bugs and provide several enhancements are now available for Red Hat Enterprise Linux 6.

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

The java-1.6.0-openjdk package has been upgraded to upstream version 1.9.7, which provides a number of bug fixes and enhancements over the previous version. (BZ#658208)

Bug Fix

BZ#659300

In Java GUI (graphical user interface) applications, placeholder characters were displayed when run in the Japanese locale. This happened because the fontconfig file defined a mapping to an unavailable font. With this update, the IPA or VLGothic fonts are mapped instead and Japanese characters are displayed correctly.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

1.112. java-1.6.0-sun

1.112.1. RHSA-2011:1384 — Critical: java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

Security Fixes

CVE-2011-3389, **CVE-2011-3516**, **CVE-2011-3521**, **CVE-2011-3544**, **CVE-2011-3545**, **CVE-2011-3546**, **CVE-2011-3547**, **CVE-2011-3548**, **CVE-2011-3549**, **CVE-2011-3550**, **CVE-2011-3551**, **CVE-2011-3552**, **CVE-2011-3553**, **CVE-2011-3554**, **CVE-2011-3555**, **CVE-2011-3556**, **CVE-2011-3557**, **CVE-2011-3558**, **CVE-2011-3560**, **CVE-2011-3561**

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide JDK and JRE 6 Update 29 and resolve these issues. All running instances of Sun Java must be restarted for the update to take effect.

1.112.2. RHSA-2011:0860 — Critical: java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

Security Fixes

CVE-2011-0802, **CVE-2011-0814**, **CVE-2011-0862**, **CVE-2011-0863**, **CVE-2011-0864**, **CVE-2011-0865**, **CVE-2011-0867**, **CVE-2011-0868**, **CVE-2011-0869**, **CVE-2011-0871**, **CVE-2011-0873**

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide JDK and JRE 6 Update 26 and resolve these issues. All running instances of Sun Java must be restarted for the update to take effect.

1.113. jss

1.113.1. RHBA-2011:0621 — jss bug fix update

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

JSS is a Java binding to Network Security Services (NSS), which provides SSL/TLS network protocols and other security services in the Public Key Infrastructure (PKI) suite. JSS is primarily utilized by the Certificate Server.

Bug Fixes

BZ#656094

With this update, JSS has been upgraded to upstream version 4.2.6, which provides a number of bug fixes over the previous version. This rebase is necessary to support the Certificate Server.

BZ#676179

Previously, JSS did not release a PK11 slot. Due to this problem, a resource leak occurred and prevented NSS from shutting down because NSS detected that resources were still in use. This update corrects the resource leak and allows NSS to shutdown.

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

1.114. kabi-whitelists

1.114.1. RHEA-2011:0797 — kabi-whitelists enhancement update

An updated kabi-whitelists package that adds two enhancements is now available for Red Hat Enterprise Linux 6.

The kabi-whitelists package contains reference files documenting interfaces provided by the Red Hat Enterprise Linux 6 kernel that are considered to be stable by Red Hat kernel engineering, and safe for longer term use by third party loadable device drivers, as well as for other purposes.

Enhancements

BZ#636975

This update removes the "blk_queue_ordered" and the "blk_queue_physical_block_size" symbols from the Red Hat Enterprise Linux 6.0 kernel ABI whitelists.

BZ#682967

This update adds several newly approved interfaces to the kernel ABI whitelists.

Note: It is not necessary to install the kabi-whitelists package in order to use Driver Updates. The kabi-whitelists package only provides reference files for use by those creating Driver Update packages, or for those who wish to enable support for verification of kernel ABI compatibility by installing the appropriate Yum plugin.

Users of kabi-whitelists are advised to upgrade to this updated package, which adds these enhancements.

1.115. kdelibs

1.115.1. RHSA-2011:1364 — Moderate: kdelibs security and enhancement update

Updated kdelibs packages that fix one security issue and add one enhancement are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having 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 kdelibs packages provide libraries for the K Desktop Environment (KDE).

Security Fix

CVE-2011-3365

An input sanitization flaw was found in the KSSL (KDE SSL Wrapper) API. An attacker could supply a specially-crafted SSL certificate (for example, via a web page) to an application using KSSL, such as the Konqueror web browser, causing misleading information to be presented to the user, possibly tricking them into accepting the certificate as valid.

Enhancement

BZ#743951

kdelibs provided its own set of trusted Certificate Authority (CA) certificates. This update makes kdelibs use the system set from the ca-certificates package, instead of its own copy.

Users should upgrade to these updated packages, which contain backported patches to correct this issue and add this enhancement. The desktop must be restarted (log out, then log back in) for this update to take effect.

1.115.2. RHSA-2011:1385 — Moderate: kdelibs and kdelibs3 security update

Updated kdelibs packages for Red Hat Enterprise Linux 4 and 5 and updated kdelibs3 packages for Red Hat Enterprise Linux 6 that fix one security issue are now available.

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 kdelibs and kdelibs3 packages provide libraries for the K Desktop Environment (KDE).

Security Fix

CVE-2011-3365

An input sanitization flaw was found in the KSSL (KDE SSL Wrapper) API. An attacker could supply a specially-crafted SSL certificate (for example, via a web page) to an application using KSSL, such as the Konqueror web browser, causing misleading information to be presented to the user, possibly tricking them into accepting the certificate as valid.

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

1.116. kernel

1.116.1. RHBA-2012:1197 — kernel bug fix update

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

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

When an NTP server asserts the STA_INS flag (Leap Second Insert), the kernel starts an hrtimer (high-resolution timer) with a countdown clock. This hrtimer expires at end of the current month, midnight UTC, and inserts a second into the kernel timekeeping structures. A scheduled leap second occurred on June 30 2012 midnight UTC.

Bug Fixes

BZ#840948

Previously in the kernel, when the leap second hrtimer was started, it was possible that the kernel livelocked on the xtime_lock variable. This update fixes the problem by using a mixture of separate subsystem locks (timekeeping and ntp) and removing the xtime_lock variable, thus avoiding the livelock scenarios that could occur in the kernel.

BZ#847364

After the leap second was inserted, applications calling system calls that used futexes consumed almost 100% of available CPU time. This occurred because the kernel's timekeeping structure update did not properly update these futexes. The futexes repeatedly expired, re-armed, and then expired immediately again. This update fixes the problem by properly updating the futex expiration times by calling the clock_was_set_delayed() function, an interrupt-safe method of the clock_was_set() function.

All users are advised to upgrade to these updated packages, which fix these bugs. The system must be rebooted for this update to take effect.

1.116.2. RHBA-2012:1310 — kernel bug fix and enhancement update

Updated kernel packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6 Extended Update Support.

[Updated 23 Oct 2012] This advisory has been updated with an accurate value of the clock drift for BZ#853951 (+/- 20 MHz). This update does not change the packages in any way.

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

Bug Fixes

BZ#844943

Prior to this update, the find_busiest_group() function used sched_group->cpu_power in the denominator of a fraction with a value of 0. Consequently, a kernel panic occurred. This update prevents the divide by zero in the kernel and the panic no longer occurs.

BZ#846830

Previously, the TCP socket bound to NFS server contained a stale skb_hints socket buffer. Consequently, kernel could terminate unexpectedly. A patch has been provided to address this issue and skb_hints is now properly cleared from the socket, thus preventing this bug.

BZ#853255

Previously, when a server attempted to shut down a socket, the svc_tcp_sendto() function set the XPT_CLOSE variable if the entire reply failed to be transmitted. However, before XPT_CLOSE could be acted upon, other threads could send further replies before the socket was really shut down. Consequently, data corruption could occur in the RPC record marker. With this update, send operations on a closed socket are stopped immediately, thus preventing this bug.

BZ#853951

When a PIT (Programmable Interval Timer) MSB (Most Significant Byte) transition occurred very close to an SMI (System Management Interrupt) execution, the pit_verify_msb() function did not see the MSB transition. Consequently, the pit_expect_msb() function returned success incorrectly, eventually causing a large clock drift in the quick_pit_calibrate() function. As a result, the TSC (Time Stamp Counter) calibration on some systems was off by +/- 20 MHz, which led to inaccurate timekeeping or ntp synchronization failures. This update fixes pit_expect_msb() and the clock drift no longer occurs in the described scenario.

Enhancement

BZ#847731

This update adds support for the Proportional Rate Reduction (PRR) algorithms for the TCP protocol. This algorithm determines TCP's sending rate in fast recovery. PRR avoids excessive window reductions and improves accuracy of the amount of data sent during loss recovery. In addition, a number of other enhancements and bug fixes for TCP are part of this update.

All users are advised to upgrade to these updated packages, which fix these bugs and add this enhancement. The system must be rebooted for this update to take effect.

1.116.3. RHBA-2013:0240 — 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#891859

On Red Hat Enterprise Linux 6, mounting an NFS export from a Windows 2012 server failed due to the fact that the Windows server contains support for the minor version 1 (v4.1) of the NFS version 4 protocol only, along with support for versions 2 and 3. The lack of the minor version 0 (v4.0) support caused Red Hat Enterprise Linux 6 clients to fail instead of rolling back to version 3 as expected. This update fixes this bug and mounting an NFS export works as expected.

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.

1.116.4. RHSA-2011:0542 — Important: Red Hat Enterprise Linux 6.1 kernel security, bug fix and enhancement update

IMPORTANT

This update has already been released as the security errata RHSA-2011:0542

Updated kernel packages that fix multiple security issues, address several hundred bugs, and add numerous enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 6. This is the first regular update.

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
* Multiple 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 Ethernet bonding driver implementation. Packets coming in from network devices that have more than 16 receive queues to a bonding interface could cause a denial of service. (CVE-2011-1581, 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, 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 was found in the transmit methods (xmit) for the loopback and InfiniBand transports in the Linux kernel's Reliable Datagram Sockets (RDS) implementation. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2011-1023, 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)

* 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)

Red Hat would like to thank Dan Rosenberg for reporting CVE-2011-1494 and CVE-2011-1495; Nelson Elhage for reporting CVE-2011-1082; Timo Warns for reporting CVE-2011-1010 and CVE-2011-1163; and Vasiliy Kulikov for reporting CVE-2011-1170, CVE-2011-1171, and CVE-2011-1172.

Bug Fixes

BZ#622327

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#640576

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#640579

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#640611

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#642570

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#646384

Running certain workload tests on a Non-Uniform Memory Architecture (NUMA) 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#622640

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#637332

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#696337

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 problems have been fixed and a bond interface works as expected.

BZ#609516

Booting a system via the Extensible Firmware Interface (EFI) could result in a low resolution of the boot screen due to a VGA palette corruption. With this update, the VGA palette corruption no longer occurs and the boot screen is displayed in the correct resolution and colors.

BZ#626454

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#640870

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

BZ#640871

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#644896

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.

BZ#530618

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.

BZ#681017

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#624628

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#628805

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#634232

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#635535

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#643750

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#643751

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#605786

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) is deprecated.

BZ#675102

Prior to this update, the /usr/include/linux/fs.h file was broken, causing other packages to fail to build. With this update, the underlying source code has been modified to address this issue, and packages no longer fail to build.

BZ#629178

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#616296

While not mandated by any specification, Linux systems rely on NMIs (Non-maskable Interrupts) being blocked by an IF-enabling (Interrupt Flag) STI instruction (an x86 instruction that enables interrupts; Set Interrupts); 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#645898

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#626814

In some cases the NFS server fails to notify NFSv4 clients about renames and unlinks done by other clients, or by non-NFS users of the server. An application on a client may then be able to open the file at its old pathname (and read old cached data from it, and perform read locks on it), long after the file no longer exists at that pathname on the server. To work around this issue, use NFSv3 instead of NFSv4. Alternatively, turn off support for leases by writing ***0*** to **`/proc/sys/fs/leases-enable`** (ideally on boot, before the nfs server is started). This change prevents NFSv4 delegations from being given out, restoring correctness at the expense of some performance.

BZ#695488

In a four node cluster environment, a deadlock could occur on machines in the cluster when the nodes accessed a GFS2 file system. This resulted in memory fragmentation which caused the number of network packet fragments in requests to exceed the network hardware limit. The network hardware firmware dropped the network packets exceeding this limit. With this update, the network packet fragmentation was reduced to the limit of the network hardware, no longer causing problems during memory fragmentation.

BZ#627741

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#647365

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#668470

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#636678

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#635710

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.

BZ#695478

The driver for the NetXen NX3031 network adapter did not support more than 14 fragments for a non-TSO (TCP Segmentation Offload) packet, which could have caused network failures. This update corrects the driver.

BZ#641764

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#632021

If a Xen guest which specifies a physical path such as /dev/sda1 in its /etc/fstab configuration file, instead of a labeled path, then the following workaround procedure should be followed:

1. The "xen_emul_unplug=never" option should be added to the guest's kernel boot line.
2. The /etc/fstab entry should be modified to specify a partition such as /dev/xvda1 for the /boot partition, or a proper partition label should be used for the file systems on the emulated block device.
3. Finally, if the Xen guest configuration spec uses a line similar to the following:

   ```
   disk = [ 'file:/var/lib/xen/images/rhel6-guest.dsk,hda,w', ]
   ```

   …then that line should be changed to:

   ```
   disk = [ 'tap:aio:/var/lib/xen/images/rhel6-guest.dsk,hda,w', ]
   ```

   This line needs to be changed because the Xen para-virtualized disk driver is not supported with file-backed I/O.

BZ#680126

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#625914

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#631547

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#698016

When the iscsi driver detected the platform option-rom, it bypassed its local defaults and used the platform-provided parameters. With this update, if the platform specifies invalid OEM parameters, a warning message is printed, and the iSCSI driver falls back on its sensible internal default parameters rather than failing to load the driver altogether.

BZ#694106

After a raid45->raid0 takeover operation, another takeover operation (for example, raid0->raid5) resulted in kernel panic. This was due to the 'degraded' and 'plug' variables from the mddev structure not being cleared after the raid4->raid0 takeover. With this update, aforementioned variables are properly cleared, and no longer cause kernel panic.

BZ#550724

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#643371

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#645198

The Red Hat Enterprise Linux kernel can now be tainted with a "tech preview" status. If a kernel module causes the tainted status, then running the command "cat /proc/modules" will display a "(T)" next to any module that is tainting the kernel.

For more information about Technology Previews, refer to:

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

IMPORTANT

Running a kernel with the tainted flag set may limit the amount of support that Red Hat can provide for the system.

BZ#694913

The "perf" subsystem failed to load on HP ProLiant servers, and messages similar to the following were logged to the console at boot time:

```
NMI watchdog disabled for cpu1: unable to create perf event: -2
```

This update includes a patch that allows the "perf" subsystem to load when using these servers, but only using the same counter that the BIOS uses. The implications of this are that "perf" statistics could be corrupted.

BZ#643667

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#615309

Direct Asynchronous I/O (AIO) which is not issued on file system block boundaries, and falls into a hole in a sparse file on ext4 or xfs file systems, may corrupt file data if multiple I/O operations modify the same file system block. Specifically, if qemu-kvm is used with the aio=native I/O mode over a sparse device image hosted on the ext4 or xfs filesystem, guest file system corruption will occur if partitions are not aligned with the host file system block size. This issue can be avoided by using one of the following techniques:

1. Align AIOs on file system 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 file system block boundary (default 4k).

BZ#624909

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#593766

The /var/log/messages file could have slowly filled up with error messages similar to the following:

```
ACPI Error: Illegal I/O port address/length above 64K:
0x0000000000400020/4 (20090903/hwvalid-154)
ACPI Exception: AE_LIMIT, Returned by Handler for [SystemIO]
(20090903/evregion-424)
ACPI Error (psparse-0537): Method parse/execution failed [\_GPE._L09]
(Node ffff8800797cd298), AE_LIMIT
ACPI Exception: AE_LIMIT, while evaluating GPE method [_L09]
(20090903/evgpe-568)
```

This error message no longer occurs with this update.

BZ#653245

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#627653

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#659480

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#621304

The RELEASE_LOCKOWNER operation has been implemented for the NFSv4 client in order to avoid an exhaustion of NFS server state IDs, which could result in an NFS4ERR_RESOURCE error. Additionally, this update introduces NFSv4 lock state tracking in read/write requests and lock owners labeling.

BZ#626515

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#661113

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#630810

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#629066

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#629836

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#629085

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#641408

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#623199

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#683496

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#592879

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#613812

This update provides a number of patches that resolve a mutual exclusion fault which could cause the kernel to become unresponsive.

BZ#634500

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#619818

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

BZ#633907

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#633915

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#636233

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#636771

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#638297

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#643237

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#668114

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#632631

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#635199

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.

BZ#636994

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#637805

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, resolving the possible risks.

BZ#638525

Previously, the /proc/maps file which is read by LVM2 (Logical Volume Manager) contained inconsistencies.

BZ#644380

Running the Virtual Desktop Server Manager (VDSM) and performing an lvextend 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 by a faulty use of a lock. With this update, performing an lvextend operation works as expected.

BZ#658293

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#669411

Deleting an 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#670572

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.

BZ#680140

Deleting an 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#647367

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#676579

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.

BZ#626956

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#631246

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#641315

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#665110

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#672937

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#680478

The kdump kernel (the second kernel) could in some cases become unresponsive due to a pending IPI (Inter-processor Interrupt) from the first kernel. The kernel tries to handle the IPI, but fails to do so due to a NULL pointer dereference. With this update, the underlying source code has been modified to address this issue, and kdump no longer hangs.

BZ#625585

Physical CPU Hotplug is not supported on Red Hat Enterprise Linux 6 i686.

BZ#681870

A Peripheral Component Interconnect Express (PCIe) Active State Power Management (ASPM) was not being properly enabled on some platforms. This resulted in the system becoming unresponsive and followed by a Non-Maskable Interrupt (NMI) on some HP ProLiant systems in the Hewlett Packard Smart Array (HPSA) or on some network cards. With this update, the underlying source code has been modified to address this issue.

BZ#694891

Intel Xeon processor E7 family processors have an issue in which some c-state transitions can cause false correctable Machine Check Exception (MCE) errors to be reported from MCE bank 6 to the user. On some E7 processor family systems, this resulted in "floods" of MCE errors. This patch disables MCE error reporting for bank 6.

BZ#634703

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#651584

Kernel panic could occur when the gfs2_glock_hold function was called within the gfs2_process_unlinked_inode function. This was due to the fact that gfs2_glock_hold was being called without a reference already held on the inode in question. This update, resolves this problem by changing the order in which it acquires references to match that of the NFS code; thus, kernel panic no longer occurs.

BZ#695751

A previously applied patch accidentally removed a check that handled invalid EEPROM (Electrically Erasable Programmable Read-Only Memory) sizes. Without this check the EEPROM validation failed if the EEPROM size was invalid, causing the NIC (Network Interface Controller) to not function properly. This update reintroduces the aforementioned patch, fixing the problem.

BZ#628951

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#636978

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#676640

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#678099

A race condition could occur during a threaded coredump causing some threads to not have a full register set. With this update, the underlying source code has been modified to address this issue and prevent the aforementioned race condition.

BZ#681668

If an EEH (Enhanced I/O Error Handling) error occurred too early in the boot process, the kernel panicked with an error message similar to the following:

```
Unable to handle kernel paging request for data at address 0x00000468
Oops: Kernel access of bad area, sig: 11 [#1]
```

- This situation is detected and avoided with this update, with the result that the machine continues to boot normally.

BZ#683115

A race condition caused by a missing mutual exclusion lock in the device_pm_pre_add() function and the device_pm_pre_add_cleanup() function could occur during the booting of an IBM Power system. As a result, error diagnostic messages were displayed in dmesg. This update adds the missing mutual exclusion lock, resolving this issue.

BZ#684961

On the PowerPC architecture, a PCI adapter with two functions, one of which uses MSI (Message Signaled Interrupts), and one of which uses MSI-X (an extended version of MSI), could have triggered an EEH (Enhanced I/O Error Handling) from an MSI-X signal when MSI was disabled using an older interface. With this update, the newer interface is used to disable MSI, with the result that the adapter no longer signals a stray MSI-X interrupt, and no EEH is registered.

BZ#694327

A previously released patch added a spin_unlock into the dtl_disable function for the virtual processor dispatch trace log file. However, the dtl_function did not include a spin_unlock which could cause a deadlock to occur. With this update, the missing spin_unlock has been added, and a deadlock no longer occurs.

BZ#695678

Section 14.11.3.2 "H_REGISTER_VPA" in the POWER Architecture Platform Reference (PAPR) specified that Dispatch Trace Log (DTL) buffers could not cross Active Memory Sharing (AMS) environments and memory entitlement granule boundaries (of size 4kB). However, kmalloc (a method for allocating memory in the kernel) did not guarantee an alignment of the allocation beyond 8 bytes. This update adds a special kmem cache for DLT buffers with the aforementioned alignment requirement.

BZ#593566

Certain scan requests failed to complete before the network interface was brought down. As a result, a warning will appear in the kernel log regarding wdev_cleanup_work. In some cases connectivity may be lost until the next reboot. If connectivity is restored, then the warning may be safely ignored. In other cases, the driver module may need to be reloaded or the system may need to be rebooted.

BZ#633836

Installing a debug kernel caused the PERC (Dell PowerEdge RAID Controller) 700 adapter to enter an undefined state and produce incorrect error messages. This has been corrected so that installing the debug kernel no longer causes the PERC 700 adapter to enter an undefined state and display erroneous RAID DIMM error messages.

BZ#664832

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#692673

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.

BZ#638269

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#680549

Previously, the UDP (User Datagram Protocol) transmit path ran under a socket lock due to the corking feature, which limited scalability due to having to transmit to the same socket in multiple threads. With this update, the transmit path has been made lockless when corking is not used, which greatly increases UDP transmit speed.

BZ#630060

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

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

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

BZ#700430

Under certain circumstances, a command could be left unprocessed when using either the cciss or the hpsa driver. This was because the HP Smart Array controller considered all commands to be completed when, in fact, some commands were still left in the completion queue. This could cause the file system to become read-only or panic and the whole system to become unstable. With this update, an extra read operation has been added to both of the aforementioned drivers, fixing this issue.

BZ#617137

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#664364

Invocating 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#655231

A previously introduced patch that prevented kbuild to attempt to sign an out-of-the-tree module only fixed this issue for cases when a full kernel tree was used for compiling. Using the kernel-devel package for compilation remained broken. This update allows out-of-the-tree modules to compile using the kernel-devel package only.

BZ#703504

Prior to this update, external modules could be built using the "-Werr" option, which resulted in a failure to build any major third party module. This update, disables the "-Werr" option for external modules, fixing the issue.

Enhancements

BZ#628676

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#629205

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#636922

The ALSA HDA audio driver has been updated to improve support for new chipsets and HDA audio codecs.

BZ#693050

The **`perf`** subsystem's **`trace`** command has been replaced with the **`script`** command. Users should now use the **`script`** command.

BZ#633571

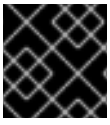
This update provides VLAN null tagging support (VLAN ID 0 can be used in tags).

BZ#591796, BZ#591797, BZ#624615, BZ#637237

USB 3.0 support has been changed from Technology Preview to full support, and supports Power Management as well as other chips other than NEC.

Users should upgrade to these updated packages, which contain backported patches to correct these issues, fix these bugs, and add these enhancement. The system must be rebooted for this update to take effect.

1.116.5. RHSA-2011:0836 — Important: kernel security and bug fix update



IMPORTANT

This update has already been released as the security errata RHSA-2011:0836

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
* An integer underflow flaw, leading to a buffer overflow, was found in the Linux kernel's Datagram Congestion Control Protocol (DCCP) implementation. This could allow a remote attacker to cause a denial of service. (CVE-2011-1770, Important)

* Missing sanity checks were found in **`setup_arg_pages()`** in the Linux kernel. When making the size of the argument and environment area on the stack very large, it could trigger a **`BUG_ON()`**, resulting in a local denial of service. (CVE-2010-3858, Moderate)

* A missing validation check was found in the **`bcm_release()`** and **`raw_release()`** functions in the Linux kernel's Controller Area Network (CAN) implementation. This could allow a local, unprivileged user to cause a denial of service. (CVE-2011-1598, CVE-2011-1748, Moderate)

* The fix for Red Hat Bugzilla bug 656461, as provided in RHSA-2011:0542, introduced a regression in the **`cifs_close()`** function in the Linux kernel's Common Internet File System (CIFS) implementation. A local, unprivileged user with write access to a CIFS file system could use this flaw to cause a denial of service. (CVE-2011-1771, Moderate)

Red Hat would like to thank Dan Rosenberg for reporting CVE-2011-1770; Brad Spengler for reporting CVE-2010-3858; and Oliver Hartkopp for reporting CVE-2011-1748.

Bug Fixes

BZ#704000

This update includes two fixes for the **`bna`** driver, specifically:

- A memory leak was caused by an unintentional assignment of the NULL value to the RX path destroy callback function pointer after a correct initialization.
- During a kernel crash, the **`bna`** driver control path state machine and firmware did not receive a notification of the crash, and, as a result, were not shut down cleanly.

BZ#704002

This update adds a missing patch to the **`ixgbe`** driver to use the kernel's generic routine to set and obtain the DCB (Data Center Bridging) priority. Without this fix, applications could not properly query the DCB priority.

BZ#704009

Prior to this update, the interrupt service routine was performing unnecessary MMIO operation during performance testing on IBM POWER7 machines. With this update, the logic of the routine has been modified so that there are fewer MMIO operations in the performance path of the code. Additionally, as a result of the aforementioned change, an existing condition was exposed where the IPR driver (the controller device driver) could return an *unexpected* HRRQ (Host Receive Request) interrupt. The original code flagged the interrupt as *unexpected* and then reset the adapter. After further

analysis, it was confirmed that this condition could occasionally occur and the interrupt can be safely ignored. Additional code provided by this update detects this condition, clears the interrupt, and allows the driver to continue without resetting the adapter.

BZ#704011

After receiving an ABTS response, the FCoE (Fibre Channel over Ethernet) DDP error status was cleared. As a result, the FCoE DDP context invalidation was incorrectly bypassed and caused memory corruption. With this update, the underlying source code has been modified to address this issue, and memory corruption no longer occurs.

BZ#704014

The Brocade BFA FC/FCoE driver was previously selectively marked as a *Technology Preview* based on the type of the adapter. With this update, the Brocade BFA FC/FCoE driver is always marked as a *Technology Preview*.

BZ#704280

This update standardizes the printed format of UUIDs (Universally Unique Identifier)/GUIDs (Globally Unique Identifier) by using an additional extension to the **%p** format specifier (which is used to show the memory address value of a pointer).

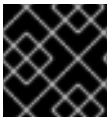
BZ#704282

The Brocade BFA FC SCSI driver (**bfa** driver) has been upgraded to version 2.3.2.4. Additionally, this update provides the following two fixes:

- A firmware download memory leak was caused by the **release_firmware()** function not being called after the **request_firmware()** function. Similarly, the firmware download interface has been fixed and now works as expected.
- During a kernel crash, the **bfa** I/O control state machine and firmware did not receive a notification of the crash, and, as a result, were not shut down cleanly.

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.

1.116.6. RHSA-2011:0928 — Important: kernel security and bug fix update



IMPORTANT

This update has already been released as the security errata RHSA-2011:0928

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

* It was found that the receive hook in the **ipip_init()** function in the **ipip** module, and in the

ipgre_init() function in the **ip_gre** module, could be called before network namespaces setup is complete. If packets were received at the time the **ipip** or **ip_gre** module was still being loaded into the kernel, it could cause a denial of service. (CVE-2011-1767, CVE-2011-1768, Moderate)

* It was found that an **mmap()** call with the ***MAP_PRIVATE*** flag on **/dev/zero** would create transparent hugepages and trigger a certain robustness check. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2011-2479, Moderate)

Bug Fixes

BZ#712413

Deleting the **lost+found** directory on a file system with inodes of size greater than 128 bytes and reusing inode 11 for a different file caused the extended attributes for inode 11 (which were set before a **umount** operation) to not be saved after a file system remount. As a result, the extended attributes were lost after the remount. With this update, inodes store their extended attributes under all circumstances.

BZ#711540

Disk read operations on a memory constrained system could cause allocations to stall. As a result, the system performance would drop considerably. With this update, latencies seen in page reclaim operations have been reduced and their efficiency improved; thus, fixing this issue.

BZ#711528

Multiple GFS2 nodes attempted to unlink, rename, or manipulate files at the same time, causing various forms of file system corruption, panics, and withdraws. This update adds multiple checks for **dinode**'s ***i_nlink*** value to assure inode operations such as link, unlink, or rename no longer cause the aforementioned problems.

BZ#711535

Migration of a Windows XP virtual guest during the early stage of a boot caused the virtual guest OS to fail to boot correctly. With this update, the underlying source code has been modified to address this issue, and the virtual guest OS no longer fails to boot.

BZ#713135

When using certain SELinux policies, such as the MLS policy, it was not possible to properly mount the **cgroupfs** file system due to the way security checks were applied to the new cgroupfs inodes during the **mount** operation. With this update, the security checks applied during the mount operation have been changed so that they always succeed, and the **cgroupfs** file system can now be successfully mounted and used with the MLS SELinux policy. This issue did not affect systems which used the default **targeted** policy.

BZ#711546

Prior to this update, Red Hat Enterprise Linux Xen (up to version 5.6) did not hide 1 GB pages and RDTSCP (enumeration features of CPUID), causing guest soft lock ups on AMD hosts when the guest's memory was greater than 8 GB. With this update, a Red Hat Enterprise Linux 6 HVM (Hardware Virtual Machine) guest is able to run on Red Hat Enterprise Linux Xen 5.6 and lower.

BZ#714190

A kernel panic in the **mpt2sas** driver could occur on an IBM system using a drive with SMART (Self-Monitoring, Analysis and Reporting Technology) issues. This was because the driver was sending an SEP request while the kernel was in the *interrupt context*, causing the driver to enter the sleep state.

With this update, a fake event is not executed from the interrupt context, assuring the SEP request is properly issued.

BZ#713494

When VLANs stacked on top of multiqueue devices passed through these devices, the ***queue_mapping*** value was not properly decremented because the VLAN devices called the physical devices via the **ndo_select_queue** method. This update removes the multiqueue functionality, resolving this issue.

BZ#713492

Prior to this update, code was missing from the **netif_set_real_num_tx_queues()** function which prevented an increment of the real number of TX queues (the ***real_num_tx_queues*** value). This update adds the missing code; thus, resolving this issue.

BZ#711524

Prior to this update, interrupts were enabled before the dispatch log for the boot CPU was set up, causing kernel panic if a timer interrupt occurred before the log was set up. This update adds a check to the **scan_dispatch_log** function to ensure the dispatch log has been allocated.

BZ#712414

Prior to this update, in the **__cache_alloc()** function, the ***ac*** variable could be changed after **cache_alloc_refill()** and the following **kmemleak_erase()** function could receive an incorrect pointer, causing kernel panic. With this update, the ***ac*** variable is updated after the **cache_alloc_refill()** unconditionally.

BZ#711520

Due to an uninitialized variable (specifically, the ***isr_ack*** variable), a virtual guest could become unresponsive when migrated while being rebooted. With this update, the said variable is properly initialized, and virtual guests no longer hang in the aforementioned scenario.

BZ#713458

A previously introduced update intended to prevent IOMMU (I/O Memory Management Unit) domain exhaustion introduced two regressions. The first regression was a race where a domain pointer could be freed while a lazy flush algorithm still had a reference to it, eventually causing kernel panic. The second regression was an erroneous reference removal for identity mapped and VM IOMMU domains, causing I/O errors. Both of these regressions could only be triggered on Intel based platforms, supporting VT-d, booted with the **intel_iommu=on** boot option. With this update, the underlying source code of the **intel-iommu** driver has been modified to resolve both of these problems. A forced flush is now used to avoid the lazy use after free issue, and extra checks have been added to avoid the erroneous reference removal.

BZ#713831

Previously, auditing system calls used a simple check to determine whether a return value was positive or negative, which also determined the success of the system call. With an exception of few, this worked on most platforms and with most system calls. For example, the 32 bit **mmap** system call on the AMD64 architecture could return a pointer which appeared to be of value **negative** even though pointers are normally of unsigned values. This resulted in the **success** field being incorrect. This patch fixes the success field for all system calls on all architectures.

BZ#709381

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#682989

Prior to this update, the **/proc/diskstats** file showed erroneous values. This occurred when the kernel merged two I/O operations for adjacent sectors which were located on different disk partitions. Two merge requests were submitted for the adjacent sectors, the first request for the second partition and the second request for the first partition, which was then merged to the first request. The first submission of the merge request incremented the **in_flight** value for the second partition. However, at the completion of the merge request, the **in_flight** value of a different partition (the first one) was decremented. This resulted in the erroneous values displayed in the /proc/diskstats file. With this update, the merging of two I/O operations which are located on different disk partitions has been fixed and works as expected.

Enhancements

BZ#711550

This updates introduces a kernel module option that allows the disabling of the Flow Director.

BZ#711548

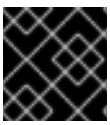
This update adds XTS (XEX-based Tweaked CodeBook) AES256 self-tests to meet the FIPS-140 requirements.

BZ#711545

This update reduces the overhead of probes provided by **kprobe** (a dynamic instrumentation system), and enhances the performance of **SystemTap**.

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add the enhancement. The system must be rebooted for this update to take effect.

1.116.7. RHSA-2011:1189 — Important: kernel security and bug fix update



IMPORTANT

This update has already been released as the security errata RHSA-2011:1189

Updated kernel packages that fix several security issues, various bugs, and add two enhancements 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
* Using PCI passthrough without interrupt remapping support allowed KVM guests to generate MSI interrupts and thus potentially inject traps. A privileged guest user could use this flaw to crash the host or possibly escalate their privileges on the host. The fix for this issue can prevent PCI passthrough working and guests starting. Refer to Red Hat Bugzilla bug 715555 for details. (CVE-2011-1898, Important)

* Flaw in the client-side NLM implementation could allow a local, unprivileged user to cause a denial of service. (CVE-2011-2491, Important)

* Integer underflow in the Bluetooth implementation could allow a remote attacker to cause a denial of service or escalate their privileges by sending a specially-crafted request to a target system via Bluetooth. (CVE-2011-2497, Important)

* Buffer overflows in the netlink-based wireless configuration interface implementation could allow a local user, who has the **`CAP_NET_ADMIN`** capability, to cause a denial of service or escalate their privileges on systems that have an active wireless interface. (CVE-2011-2517, Important)

* Flaw in the way the maximum file offset was handled for ext4 file systems could allow a local, unprivileged user to cause a denial of service. (CVE-2011-2695, Important)

* Flaw allowed **`napi_reuse_skb()`** to be called on VLAN packets. An attacker on the local network could use this flaw to send crafted packets to a target, possibly causing a denial of service. (CVE-2011-1576, Moderate)

* Integer signedness error in **`next_pidmap()`** could allow a local, unprivileged user to cause a denial of service. (CVE-2011-1593, Moderate)

* Race condition in the memory merging support (KSM) could allow a local, unprivileged user to cause a denial of service. KSM is off by default, but on systems running VDSM, or on KVM hosts, it is likely turned on by the **`ksm`**/**`ksmtuned`** services. (CVE-2011-2183, Moderate)

* Flaw in **`inet_diag_bc_audit()`** could allow a local, unprivileged user to cause a denial of service. (CVE-2011-2213, Moderate)

* Flaw in the way space was allocated in the Global File System 2 (GFS2) implementation. If the file system was almost full, and a local, unprivileged user made an **`fallocate()`** request, it could result in a denial of service. Setting quotas to prevent users from using all available disk space would prevent exploitation of this flaw. (CVE-2011-2689, Moderate)

* Local, unprivileged users could send signals via the **`sigqueueinfo`** system call, with **`si_code`** set to ***`SI_TKILL`*** and with spoofed process and user IDs, to other processes. 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)

* Heap overflow in the EFI GUID Partition Table (GPT) implementation could allow a local attacker to cause a denial of service by mounting a disk containing crafted partition tables. (CVE-2011-1776, Low)

* Structure padding in two structures in the Bluetooth implementation was not initialized properly before being copied to user-space, possibly allowing local, unprivileged users to leak kernel stack memory to user-space. (CVE-2011-2492, Low)

* **`/proc/[PID]/io`** is world-readable by default. Previously, these files could be read without any further restrictions. A local, unprivileged user could read these files, belonging to other, possibly privileged processes to gather confidential information, such as the length of a password used in a process. (CVE-2011-2495, Low)

Red Hat would like to thank Vasily Averin for reporting CVE-2011-2491; Dan Rosenberg for reporting CVE-2011-2497 and CVE-2011-2213; Ryan Sweat for reporting CVE-2011-1576; Robert Swiecki for reporting CVE-2011-1593; Andrea Righi for reporting CVE-2011-2183; Julien Tinnes of the Google Security Team for reporting CVE-2011-1182; Timo Warns for reporting CVE-2011-1776; Marek Kroemeke and Filip Palian for reporting CVE-2011-2492; and Vasiliy Kulikov of Openwall for reporting CVE-2011-2495.

Bug Fixes

BZ#719925

This update fixes a regression in which a client would use an **UNCHECKED NFS CREATE** call when an open system call was attempted with the **O_EXCL**|**O_CREAT** flag combination. An **EXCLUSIVE NFS CREATE** call should have been used instead to ensure that **O_EXCL** semantics were preserved. As a result, an application could be led to believe that it had created the file when it was in fact created by another application.

BZ#714982

In a GFS2 file system, when the responsibility for deallocation was passed from one node to another, the receiving node may not have had a fully up-to-date inode state. If the sending node has changed the important parts of the state in the mean time (block allocation/deallocation) then this resulted in triggering an assert during the deallocation on the receiving node. With this update, the inode state is refreshed correctly during deallocation on the receiving node, ensuring that deallocation proceeds normally.

BZ#720914

Prior to this update, the **ehea** driver caused a kernel oops during a memory hotplug if the ports were not up. With this update, the waitqueues are initialized during the port probe operation, instead of during the port open operation.

BZ#725329

Older versions of **be2net** cards firmware may not recognize certain commands and return illegal/unsupported errors, causing confusing error messages to appear in the logs. With this update, the driver handles these errors gracefully and does not log them.

BZ#726308

This patch fixes the inability of the **be2net** driver to work in a kdump environment. It clears an interrupt bit (in the card) that may be set while the driver is probed by the kdump kernel after a crash.

BZ#715397

The **hpsa** driver has been updated to provide a fix for **hpsa** driver **kdump** failures.

BZ#716539

Memory limit for x86_64 domU PV guests has been increased to 128 GB: **CONFIG_XEN_MAX_DOMAIN_MEMORY=128**.

BZ#726095

The patch that fixed BZ#556572 introduced a bug where the page lock was being released too soon, allowing the **do_wp_page** function to reuse the wrprotected page before PageKsm would be set in ***page->mapping***. With this update, a new version of the original fix was introduced, thus fixing this issue.

BZ#717018

While running **gfs2_grow**, the file system became unresponsive. This was due to the log not getting flushed when a node dropped its rindex glock so that another node could grow the file system. If the log did not get flushed, GFS2 could corrupt the **sd_log_le_rg** list, ultimately causing a hang. With this update, a log flush is forced when the rindex glock is invalidated; **gfs2_grow** completes as expected and the file system remains accessible.

BZ#719928

After hot plugging one of the disks of a non-boot 2-disk RAID1 pair, the **md** driver would enter an infinite resync loop thinking there was a spare disk available, when, in fact, there was none. This update adds an additional check to detect the previously mentioned situation; thus, fixing this issue.

BZ#723807

This update fixes two bugs related to **Rx** checksum offloading. These bugs caused a data corruption transferred over r8169 NIC when **Rx** checksum offloading was enabled.

BZ#719910

The 128-bit multiply operation in the **pvclock.h** function was missing an output constraint for EDX which caused a register corruption to appear. As a result, Red Hat Enterprise Linux 3.8 and Red Hat Enterprise Linux 3.9 KVM guests with a Red Hat Enterprise Linux 6.1 KVM host kernel exhibited time inconsistencies. With this update, the underlying source code has been modified to address this issue, and time runs as expected on the aforementioned systems.

Enhancements

BZ#713827

This update adds parallel port printing support for Red Hat Enterprise Linux 6.

BZ#723820

Prior to this update, the **be2net** driver was using the BE3 chipset in legacy mode. This update enables this chipset to work in a native mode, making it possible to use all 4 ports on a 4-port integrated NIC.

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements. The system must be rebooted for this update to take effect.

1.116.8. RHSA-2011:1350 — Important: kernel security, bug fix, and enhancement update

IMPORTANT

This update has already been released as the security errata RHSA-2011:1350.

Updated kernel packages that fix multiple security issues, 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

* Flaws in the **AGPGART** driver implementation when handling certain IOCTL commands could allow a local user to cause a denial of service or escalate their privileges. (CVE-2011-1745, CVE-2011-2022, Important)

* An integer overflow flaw in **agp_allocate_memory()** could allow a local user to cause a denial of service or escalate their privileges. (CVE-2011-1746, Important)

* A race condition flaw was found in the Linux kernel's eCryptfs implementation. A local attacker could use the **mount.ecryptfs_private** utility to mount (and then access) a directory they would otherwise not have access to. Note: To correct this issue, the RHSA-2011:1241 ecryptfs-utils update, which provides the user-space part of the fix, must also be installed. (CVE-2011-1833, Moderate)

* A denial of service flaw was found in the way the taskstats subsystem handled the registration of process exit handlers. A local, unprivileged user could register an unlimited amount of these handlers, leading to excessive CPU time and memory use. (CVE-2011-2484, Moderate)

* A flaw was found in the way mapping expansions were handled. A local, unprivileged user could use this flaw to cause a wrapping condition, triggering a denial of service. (CVE-2011-2496, Moderate)

* A flaw was found in the Linux kernel's Performance Events implementation. It could falsely lead the NMI (Non-Maskable Interrupt) Watchdog to detect a lockup and panic the system. A local, unprivileged user could use this flaw to cause a denial of service (kernel panic) using the perf tool. (CVE-2011-2521, Moderate)

* A flaw in **skb_gro_header_slow()** in the Linux kernel could lead to GRO (Generic Receive Offload) fields being left in an inconsistent state. An attacker on the local network could use this flaw to trigger a denial of service. GRO is enabled by default in all network drivers that support it. (CVE-2011-2723, Moderate)

* A flaw was found in the way the Linux kernel's Performance Events implementation handled **PERF_COUNT_SW_CPU_CLOCK** counter overflow. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2011-2918, Moderate)

* A flaw was found in the Linux kernel's Trusted Platform Module (TPM) implementation. A local, unprivileged user could use this flaw to leak information to user-space. (CVE-2011-1160, Low)

* Flaws were found in the **tpacket_rcv()** and **packet_recvmsg()** functions in the Linux kernel. A local, unprivileged user could use these flaws to leak information to user-space. (CVE-2011-2898, Low)

Red Hat would like to thank Vasiliy Kulikov of Openwall for reporting CVE-2011-1745, CVE-2011-2022, CVE-2011-1746, and CVE-2011-2484; the Ubuntu Security Team for reporting CVE-2011-1833; Robert Swiecki for reporting CVE-2011-2496; Li Yu for reporting CVE-2011-2521; Brent Meshier for reporting CVE-2011-2723; and Peter Huewe for reporting CVE-2011-1160. The Ubuntu Security Team acknowledges Vasiliy Kulikov of Openwall and Dan Rosenberg as the original reporters of CVE-2011-1833.

Bug Fixes

BZ#727618

When an event caused the **ibmvscsi** driver to reset its CRQ, re-registering the CRQ returned H_CLOSED, indicating that the Virtual I/O Server was not ready to receive commands. As a consequence, the **ibmvscsi** driver offlined the adapter and did not recover. With this update, the

interrupt is re-enabled after the reset so that when the Virtual I/O server is ready and sends a CRQ init, it is able to receive it and resume initialization of the VSCSI adapter.

BZ#728522

Suspending a system to RAM and consequently resuming it caused USB3.0 ports to not work properly. This was because a USB3.0 device configured for MSIX would, during the resume operation, incorrectly read its previous interrupt state. This would lead it to fall back to a legacy mode and appear unresponsive. With this update, the interrupt state is cached, allowing the driver to properly resume its previous state.

BZ#736065

Prior to this update, kdump failed to create a **`vmcore`** file after triggering a crash on POWER7 systems with Dynamic DMA Windows enabled. This update provides a number of fixes that address this issue.

BZ#713463

Prior to this update, loading the FS-Cache kernel module would cause the kernel to be tainted as a Technology Preview via the **`mark_tech_preview()`** function, which would cause kernel lock debugging to be disabled by the **`add_taint()`** function. However, the NFS and CIFS modules depend on the FS-Cache module so using either NFS or CIFS would cause the FS-Cache module to be loaded and the kernel tainted. With this update, FS-Cache only taints the kernel when a cache is brought online (for instance by starting the **`cachefilesd`** service) and, additionally, the **`add_taint()`** function has been modified so that it does not disable lock debugging for informational-only taints.

BZ#723551

A race between the **`FSFREEZE`** **`ioctl()`** command to freeze an ext4 file system and **`mmap`** I/O operations would result in a deadlock if these two operations ran simultaneously. This update provides a number of patches to address this issue, and a deadlock no longer occurs in the previously-described scenario.

BZ#710047

If a user configured 2 logical disks on a RAID volume, whose disks are larger than 2 TB, where the start of the second logical disk is after the 2 TB mark, and FastPath was enabled, FastPath reads to the second logical disk were read from the incorrect location on the disk. However, writes were not affected and always went to the correct disk location. With this update, the driver detects the **`LBA > 0xffffffff & cdb_len < 16`** condition, then converts the CDB from the OS to a 16 byte CDB, before firing it as a FastPath I/O operation.

BZ#727838

A Windows Server 2008 32-bit guest installation failed on a Red Hat Enterprise Linux 6.1 Snap2 KVM host when allocating more than one virtual CPU (***`vcpus > 1`***) during the installation. As soon the installation started after booting from ISO, a blue screen with the following error occurred:

```
A problem has been detected and windows has been shut down to prevent
damage to your computer.
```

This was because a valid microcode update signature was not reported to the guest. This update fixes this issue by reporting a non-zero microcode update signature to the guest.

BZ#732379

Prior to this update, the following message appeared in kernel log files:

```
[bnx2x_extract_max_cfg:1079(eth11)]Illegal configuration detected for
Max BW - using 100 instead
```

The above message appeared on **bnx2x** interfaces in the multi-function mode which were not used and had no link, thus, not indicating any actual problems with connectivity. With this update, the message has been removed and no longer appears in kernel log files.

BZ#726626

Previously, the **inet6_sk_generic()** function was using the ***obj_size*** variable to compute the address of its inner structure, causing memory corruption. With this update, the **sk_alloc_size()** is called every time there is a request for allocation, and memory corruption no longer occurs.

BZ#739477

Due to the partial support of IPv6 multicast snooping, IPv6 multicast packets may have been dropped. This update fixes IPv6 multicast snooping so that packets are no longer dropped.

Enhancement

BZ#732382

With this update, the JSM driver has been updated to support for enabling the Bell2 (with PLX chip) 2-port adapter on POWER7 systems. Additionally, EEH support has been added for to JSM driver.

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add the enhancement. The system must be rebooted for this update to take effect.

1.116.9. RHSA-2011:1465 — Important: kernel security and bug fix update

IMPORTANT

This update has already been released as the security errata RHSA-2011:1465.

Updated kernel packages that fix multiple security issues and various bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having 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

* IPv6 fragment identification value generation could allow a remote attacker to disrupt a target system's networking, preventing legitimate users from accessing its services. (CVE-2011-2699, Important)

* A signedness issue was found in the Linux kernel's CIFS (Common Internet File System) implementation. A malicious CIFS server could send a specially-crafted response to a directory read request that would result in a denial of service or privilege escalation on a system that has a CIFS share mounted. (CVE-2011-3191, Important)

* A flaw was found in the way the Linux kernel handled fragmented IPv6 UDP datagrams over the bridge with UDP Fragmentation Offload (UFO) functionality on. A remote attacker could use this flaw to cause a denial of service. (CVE-2011-4326, Important)

* The way IPv4 and IPv6 protocol sequence numbers and fragment IDs were generated could allow a man-in-the-middle attacker to inject packets and possibly hijack connections. Protocol sequence numbers and fragment IDs are now more random. (CVE-2011-3188, Moderate)

* A buffer overflow flaw was found in the Linux kernel's FUSE (Filesystem in Userspace) implementation. A local user in the fuse group who has access to mount a FUSE file system could use this flaw to cause a denial of service. (CVE-2011-3353, Moderate)

* A flaw was found in the **b43** driver in the Linux kernel. If a system had an active wireless interface that uses the **b43** driver, an attacker able to send a specially-crafted frame to that interface could cause a denial of service. (CVE-2011-3359, Moderate)

* A flaw was found in the way CIFS shares with DFS referrals at their root were handled. An attacker on the local network who is able to deploy a malicious CIFS server could create a CIFS network share that, when mounted, would cause the client system to crash. (CVE-2011-3363, Moderate)

* A flaw was found in the way the Linux kernel handled VLAN 0 frames with the priority tag set. When using certain network drivers, an attacker on the local network could use this flaw to cause a denial of service. (CVE-2011-3593, Moderate)

* A flaw in the way memory containing security-related data was handled in **`tpm_read()`** could allow a local, unprivileged user to read the results of a previously run TPM command. (CVE-2011-1162, Low)

* A heap overflow flaw was found in the Linux kernel's EFI GUID Partition Table (GPT) implementation. A local attacker could use this flaw to cause a denial of service by mounting a disk that contains specially-crafted partition tables. (CVE-2011-1577, Low)

* The I/O statistics from the taskstats subsystem could be read without any restrictions. A local, unprivileged user could use this flaw to gather confidential information, such as the length of a password used in a process. (CVE-2011-2494, Low)

* It was found that the **`perf`** tool, a part of the Linux kernel's Performance Events implementation, could load its configuration file from the current working directory. If a local user with access to the **`perf`** tool were tricked into running **`perf`** in a directory that contains a specially-crafted configuration file, it could cause **`perf`** to overwrite arbitrary files and directories accessible to that user. (CVE-2011-2905, Low)

Red Hat would like to thank Fernando Gont for reporting CVE-2011-2699; Darren Lavender for reporting CVE-2011-3191; Dan Kaminsky for reporting CVE-2011-3188; Yogesh Sharma for reporting CVE-2011-3363; Gideon Naim for reporting CVE-2011-3593; Peter Huewe for reporting CVE-2011-1162; Timo Warns for reporting CVE-2011-1577; and Vasiliy Kulikov of Openwall for reporting CVE-2011-2494.

Bug Fixes

BZ#734774

When a host was in recovery mode and a SCSI scan operation was initiated, the scan operation failed and provided no error output. This bug has been fixed and the SCSI layer now waits for recovery of the host to complete scan operations for devices.

BZ#737570

While executing a multi-threaded process by multiple CPUs, page-directory-pointer-table entry (PDPTE) registers were not fully flushed from the CPU cache when a Page Global Directory (PGD) entry was changed in x86 Physical Address Extension (PAE) mode. As a consequence, the process

failed to respond for a long time before it successfully finished. With this update, the kernel has been modified to flush the Translation Lookaside Buffer (TLB) for each CPU using a page table that has changed. Multi-threaded processes now finish without hanging.

BZ#740352

When a CPU is about to modify data protected by the RCU (Read Copy Update) mechanism, it has to wait for other CPUs in the system to pass a quiescent state. Previously, the guest mode was not considered a quiescent state. As a consequence, if a CPU was in the guest mode for a long time, another CPU had to wait a long time in order to modify RCU-protected data. With this update, the rcu_virt_note_context_switch() function, which marks the guest mode as a quiescent state, has been added to the kernel, thus resolving this issue.

BZ#741167

A workaround to the megaraid_sas driver was provided to address an issue but as a side effect of the workaround, megaraid_sas stopped to report certain enclosures, CD-ROM drives, and other devices. The underlying problem for the issue has been fixed as reported in BZ#741166. With this update, the original workaround has been reverted, and megaraid_sas now reports many different devices as before.

BZ#741166

Previously, some enclosure devices with a broken firmware reported incorrect values. As a consequence, kernel sometimes terminated unexpectedly. A patch has been provided to address this issue, and the kernel crashes no longer occur even if an enclosure device reports incorrect or duplicate data.

BZ#741704

During connection shut down or reconnection, the iSCSI software initiator module, iscsi_tcp, was setting callbacks to the NULL value and freeing connections while the network layer was still using the callbacks. As a consequence, kernel terminated unexpectedly. A patch has been provided to address this issue and the crashes no longer occur in the described scenario.

BZ#743510

When a SCTP (Stream Control Transmission Protocol) packet contained two COOKIE_ECHO chunks and nothing else, the SCTP state machine disabled output processing for the socket while processing the first COOKIE_ECHO chunk, then lost the association and forgot to re-enable output processing for the socket. As a consequence, any data which needed to be sent to a peer were blocked and the socket appeared to be unresponsive. With this update, a new SCTP command has been added to the kernel code, which sets the association explicitly; the command is used when processing the second COOKIE_ECHO chunk to restore the context for SCTP state machine, thus fixing this bug.

BZ#743807

Some system vendors desired the Wake-on-Lan capability to be accessible on more than the first on-board port of an Intel i350 network adapter. Due to a bug in the igb driver, this was not possible. This bug has been fixed and igb now honors the EEPROM setting for the second port.

BZ#745413

When a kernel NFS server was being stopped, kernel sometimes terminated unexpectedly. A bug has been fixed in the wait_for_completion_interruptible_timeout() function and the crashes no longer occur in the described scenario.

BZ#745557

The ACPI (Advanced Control and Power Interface) core places all events to the kacpi_notify queue including PCI hotplug events. When the acpiphp driver was loaded and a PCI card with a PCI-to-PCI bridge was removed from the system, the code path attempted to empty the kacpi_notify queue which causes a deadlock, and the kacpi_notify thread became unresponsive. With this update, the call sequence has been fixed, and the bridge is now cleaned-up properly in the described scenario.

BZ#747868

On IBM System z, if a Linux instance with large amounts of anonymous memory runs into a memory shortage the first time, all pages on the active or inactive lists are considered referenced. This causes the memory management on IBM System z to do a full check over all page cache pages and start writeback for all of them. As a consequence, the system became temporarily unresponsive when the described situation occurred. With this update, only pages with active mappers are checked and the page scan now does not cause the hangs.

BZ#740230

When a NFS server returned more than two GETATTR bitmap words in response to the FATTR4_ACL attribute request, decoding operations of the nfs4_getfacl() function failed. A patch has been provided to address this issue and the ACLs are now returned in the described scenario.

BZ#744811

In error recovery, most SCSI error recovery stages send a TUR (Test Unit Ready) command for every bad command when a driver error handler reports success. When several bad commands pointed to a same device, the device was probed multiple times. When the device was in a state where the device did not respond to commands even after a recovery function returned success, the error handler had to wait for the commands to time out. This significantly impeded the recovery process. With this update, SCSI mid-layer error routines to send test commands have been fixed to respond once per device instead of once per bad command, thus reducing error recovery time considerably.

BZ#748808

A scenario for this bug involves two hosts, configured to use IPv4 network, and two guests, configured to use IPv6 network. When a guest on host A attempted to send a large UDP datagram to host B, host A terminated unexpectedly. With this update, the ipv6_select_ident() function has been fixed to accept the in6_addr parameter and to use the destination address in IPv6 header when no route is attached, and the crashes no longer occur in the described scenario.

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.

1.116.10. RHBA-2012:0549 — kernel bug fix update

Updated kernel packages that fix three bugs and add two enhancements 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 811298. 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 Fixes

BZ#807425

An unwanted interrupt was generated when a PCI driver switched the interrupt mechanism from the

Message Signaled Interrupt (MSI or MSI-X) to the INTx emulation while shutting down a device. Due to this, an interrupt handler was called repeatedly, and the system became unresponsive. On certain systems, the interrupt handler of Intelligent Platform Management Interface (IPMI) was called while shutting down a device on the way to reboot the system after running kdump. In such a case, soft lockups were performed repeatedly and the shutdown process never finished. With this update, the user can choose not to use MSI or MSI-X for the PCI Express Native Hotplug driver. The switching between the interrupt mechanisms is no longer performed so that the unwanted interrupt is not generated.

BZ#810453

Previously, the eth_type_trans() function was called with the VLAN device type set. If a VLAN device contained a MAC address different from the original device, an incorrect packet type was assigned to the host. Consequently, if the VLAN devices were set up on a bonding interface in Adaptive Load Balancing (ALB) mode, the TCP connection could not be established. With this update, the eth_type_trans() function is called with the original device, ensuring that the connection is established as expected.

BZ#811298

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.

Enhancements

BZ#801714

The qlge 10 Gigabit Ethernet driver for QLogic 81XX converged network adapter family has been updated to version 1.00.00.29, which provides a number of bug fixes over the previous version.

BZ#806905

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 these bugs and add these enhancements. The system must be rebooted for this update to take effect.

1.116.11. RHBA-2012:0424 — kernel bug fix update

Updated kernel packages that fix multiple 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#789912

Socket callbacks use the svc_xprt_enqueue() function to add sockets to the sp_sockets list. In normal

operation, a server thread will later take the socket off that list. Previously, on the nfsd daemon shutdown, still-running svc_xprt_enqueue() could re-add a socket to the sp_sockets list just before it was deleted. Consequently, the system could terminate unexpectedly due to memory corruption in the sunrpc module. With this update, the XPT_BUSY flag is set on every socket before shutdown and svc_xprt_enqueue() now checks this flag, thus preventing this bug.

BZ#795332

Due to a race condition, running the "ifenslave -d bond0 eth0" command to remove the slave interface from the bonding device could cause the system to crash when a networking packet was being received at the same time. With this update, the race condition has been fixed and the system no longer crashes under these circumstances.

BZ#795337

In rare cases, a BUG_ON() macro could be triggered, causing the nfsd daemon to fail. The BUG_ON() macro checked the xpt_pool field, which was not actually used for anything. This update removes both the BUG_ON() macro and the xpt_pool field, fixing the problem.

BZ#795817

An insufficiently well-designed calculation in the CPU accelerator in the previous version of the kernel packages caused an arithmetic overflow in the sched_clock() function when system uptime exceeded 208.5 days. This overflow led to a kernel panic on systems using the Time Stamp Counter (TSC) or Virtual Machine Interface (VMI) clock source. This update corrects the aforementioned calculation so that this arithmetic overflow and kernel panic can no longer occur under these circumstances.

BZ#796826

On a system that created and deleted lots of dynamic devices, the 31-bit Linux ifindex object failed to fit in the 16-bit macvtap minor range, resulting in unusable macvtap devices. The problem primarily occurred in a libvirt-controlled environment when many virtual machines were started or restarted, and caused libvirt to report the following message:

Error starting domain: cannot open macvtap tap device /dev/tap222364: No such device or address

With this update, the macvtap's minor device number allocation has been modified so that virtual machines can now be started and restarted as expected in the described scenario.

BZ#799942

The dm_mirror module can send discard requests. However, the dm_io interface did not support discard requests, and running an LVM mirror over a discard-enabled device led to a kernel panic. This update adds support for the discard requests to the dm_io interface, so that kernel panics no longer occur in the described scenario.

All users of kernel are advised to upgrade to these updated packages, which fix these bugs. The system must be rebooted for this update to take effect.

1.116.12. RHBA-2011:1846 — 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#751995

Previously, the idle_balance() function dropped or retook the rq->lock parameter, leaving the previous task vulnerable to the set_tsk_need_resched() function. Now, the parameter is cleared in setup_thread_stack() after a return from balancing and no successfully descheduled or never scheduled task has it set, thus fixing this bug.

BZ#757670

A software bug related to Context Caching existed in the Intel IOMMU support module. On some newer Intel systems, the Context Cache mode has changed from previous hardware versions, potentially exposing a Context coherency race. The bug was exposed when performing a series of hot plug and unplug operations of a Virtual Function network device which was immediately configured into the network stack, i.e., successfully performed dynamic host configuration protocol (DHCP). When the coherency race occurred, the assigned device would not work properly in the guest virtual machine. With this update, the Context coherency is corrected and the race and potentially resulting device assignment failure no longer occurs.

All users of kernel are advised to upgrade to these updated packages, which fix these bugs. The system must be rebooted for this update to take effect.

1.116.13. RHBA-2011:0874 — 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#710609

Xen guests cannot make use of all CPU features, and in some cases they are even risky to be advertised. One such feature is CONSTANT_TSC. This feature prevents the TSC (Time Stamp Counter) from being marked as unstable, which allows the sched_clock_stable option to be enabled. Having the sched_clock_stable option enabled is problematic for Xen PV guests because the sched_clock() function has been overridden with the xen_sched_clock() function, which is not synchronized between virtual CPUs. This update provides a patch, which sets all x86_power features to 0 as a preventive measure against other potentially dangerous assumptions the kernel could make based on the features, fixing this issue.

BZ#712191

Issues for which a host had older hypervisor code running on newer hardware, which exposed the new CPU features to the guests, were discovered. This was dangerous because newer guest kernels (such as Red Hat Enterprise Linux 6) may have attempted to use those features or assume certain machine behaviors that it would not be able to process because it was, in fact, a Xen guest. One such place was the intel_idle driver which attempts to use the MWAIT and MONITOR instructions. These instructions are invalid operations for a Xen PV guest. This update provides a patch, which masks the MWAIT instruction to avoid this issue.

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.

1.117. kexec-tools

1.117.1. RHBA-2011:0736 — kexec-tools bug fix update

The **kexec** fastboot mechanism allows booting a Linux kernel from the context of an already running kernel. The kexec-tools package provides the **/sbin/kexec** binary and ancillary utilities that form the user-space component of the kernel's **kexec** feature.

Bug Fixes

BZ#605411

The **kdump** crash recovery service allows users to specify a *raw device* (that is, a raw disk or partition) as a target location for core dumps. Previously, when a kernel crash occurred and a core dump was written to such a raw device, **kdump** was unable to retrieve it after a reboot. With this update, the corresponding init script has been updated to search the configured raw device for the presence of a core dump upon the service startup. Now, when the **kdump** service is started and a core dump is found on the raw device, the init script retrieves it and creates a proper **vmcore** file in a local file system.

BZ#607400

Due to various unrelated errors in the underlying source code, the **kexec** utility may not have worked properly on the SGI Altix UV architecture. This update applies a set of patches to address these issues, and **kexec** now works on this architecture as expected.

BZ#619682

Prior to this update, the **kdump.conf**(5) manual page did not provide a description of the **blacklist** directive. This update corrects this error, and the **blacklist** directive is now included in the “OPTIONS” section of the **kdump.conf**(5) manual page as expected.

BZ#626318

When running the **firstboot** application in a language other than English, certain messages regarding the configuration of the **kdump** crash recovery service were presented to a user in the original English version. This update corrects this error, and the **Kdump** section of the **firstboot** application no longer contains untranslated strings.

BZ#626606

Prior to this update, an attempt to run the **mkdumprd** utility on a system without the **/etc/modprobe.d/modprobe.conf** file caused the utility to stop responding. With this update, this error no longer occurs, and **mkdumprd** now works as expected.

BZ#626746

Due to an error in the init script, the **kdump** service did not take into account the value of the **path** option in the **/etc/kdump.conf** configuration file, and always saved the **vmcore** file to the **/var/crash/** directory. This update adapts the corresponding init script to ensure that **kdump** uses the directory specified in the configuration.

BZ#627118

In accordance with the current version of the Filesystem Hierarchy Standard (FHS), the **makedumpfile** utility is now installed in the **/usr/sbin/** directory.

BZ#627834

Previously, configuring the **kdump** service to store core dumps over a network on a system that used channel bonding or bridging caused the **mkdumprd** utility to display the following error message on the service startup:

```
Netmask is missed!
```

With this update, the underlying source code has been adapted to address this issue, and **makedumpfile** no longer displays this message when channel bonding or bridging is in use.

BZ#628817

The **kdump** crash recovery service is unable to operate in Xen environment. With this update, an attempt to start **kdump** in such an environment fails with the “Kdump is not supported on this kernel” message.

BZ#628827

The commented section of the **/etc/kdump.conf** configuration file contains the following line:

```
#core_collector cp --sparse=always
```

However, uncommenting this line without including **/bin/cp** in the initial RAM disk (that is, by using the **extra_bins** directive) would cause the **kdump** crash recovery service to fail. This update corrects this error, and the above line is now followed by **#extra_bins /bin/cp**.

BZ#630305

Due to an error in the translation, when running the **firstboot** application in the Malayalam language (that is, the **ml_IN** language code), certain keyboard shortcuts on the **Kdump** screen did not work. This update corrects the Malayalam translation of the **firstboot** application, and all shortcuts can now be used as expected.

BZ#630309

When running the **firstboot** application in the Malayalam language (that is, the **ml_IN** language code), the first paragraph on the **Kdump** screen contained an incorrect string. This update adapts the Malayalam translation of the **firstboot** application, and the **Kdump** screen is now translated correctly.

BZ#642735

Prior to this update, an attempt to start the **kdump** service on a system with a large amount of memory (that is, 1TB and more) caused **kdump** to terminate unexpectedly with a segmentation fault. With this update, the underlying source code has been adapted to address this issue, and **kdump** no longer crashes

BZ#642855

Due to an error in DHCP NAK handling, previous versions of **kdump** may have failed to resolve an IP address when storing a core dump to a remote server. This update corrects this error, and **kdump** no longer fails.

BZ#645441

Prior to this update, the **kdump** crash recovery service failed to start on IBM System x3850 X5 machines. This update applies an upstream patch that extends the size of kcore ELF headers. Now, **kdump** can be started on such machines as expected.

BZ#652191

Previously, configuring the **kdump** service to store core dumps to a remote machine over the **SSH** protocol and changing the core collector to **cp** caused it to name core dump files **vmcore.flat**, even when the **SCP** (Secure Copy) protocol was used. This update corrects this error, and **kdump** now only uses the **.flat** file extension when the **makedumpfile** utility is used as the core collector.

BZ#652724

Previously, when a system did not have enough memory to use **kdump**, the **Kdump** screen of the **firstboot** application incorrectly displayed the **Enable kdump?** check box as selected, but did not allow a user to change it. This error has been fixed, and the **Enable kdump?** check box is no longer displayed when the **kdump** service cannot be configured.

BZ#654245

When the **kdump** crash recovery service was already enabled, an attempt to use the **firstboot** application to change its configuration may have failed with the following message:

```
Insufficient memory to configure kdump!
```

This update adapts the underlying source code to verify that **kdump** is not running before displaying this message.

BZ#669655

Previously, when the root partition was mounted as a read-only file system, the **mkdumprd** utility was unable to create a temporary directory and failed to build an initial RAM disk (that is, **initrd**). This update adapts **mkdumprd** to use the **/boot/** directory in this case. As a result, mounting the root partition as a read-only file system no longer renders **mkdumprd** unable to create an initial RAM disk.

BZ#671013

Due to an error in the **mkdumprd** utility, updating a disk drive firmware could render the **kdump** crash recovery service unable to recognize the disk drive. This update adapts the **mkdumprd** utility to ignore disk drive firmware revisions, and **kdump** now works as expected.

BZ#674893

Due to known issues with the **hpsa** and **cciss** drivers, **kdump** is unable to save core dumps to certain HP Smart Array Controllers that use these drivers. This update ensures that the **kdump** service is disabled on such controllers.

BZ#676758

Prior to this update, an attempt to boot a system with the new syntax of the **crashkernel** kernel parameter (such as **crashkernel=4G-:256M**) caused the **firstboot** application to terminate unexpectedly during the configuration of **kdump**. This update applies a patch to address this issue, and **firstboot** no longer crashes.

BZ#679310

When using the Russian translation (that is, the **ru_RU** language code) of the **firstboot** application, the first paragraph on the **Kdump** screen incorrectly contained the – string. This update corrects this error, and the **Kdump** section of the **firstboot** application is now translated correctly.

BZ#680741

Prior to this update, running the **makedumpfile -V** command caused the **makedumpfile** utility to terminate unexpectedly with a segmentation fault. This update applies an upstream patch that removes **-V** from the list of supported command line options, and running the above command no longer causes **makedumpfile** to crash.

BZ#683713

Due to a typing error in the underlying source code of the **mkdumprd** utility, configuring the **kdump** service to store core dumps to a raw device caused it to display a message similar to the following when a kernel crash occurred:

```
kill: cannot kill pid 887: No such process
```

This update corrects this error, and **kdump** no longer display the above error message upon a kernel crash.

BZ#683735

When configured to use a raw device as a target location for core dumps, the **kdump** service recovers the dump file at next startup. Previously, an attempt to use this configuration without the **core_collector** option specified in the configuration file caused **kdump** to fail to recover the core dump. With this update, the underlying source code has been adapted to use the **makedumpfile** utility by default, and **kdump** is now able to recover core dumps as expected.

BZ#688150

When the **firstboot** application is used to configure the **kdump** crash recovery service, a dialog box appears and prompts a user to reboot the system in order for the changes to take effect. Previously, closing this dialog box by clicking the **Close** button had the same effect as clicking **Yes**, and incorrectly initiated the system restart. This error no longer occurs, and clicking the **Close** button now only closes the dialog box as expected.

BZ#691632

Under certain circumstances, the **kdump** service may have failed to create a core dump with the following error:

```
readmem: Can't read the dump memory(/proc/vmcore). Cannot allocate
memory
```

This update fixes this regression, and **kdump** no longer fails to store the core dump.

BZ#692264

Prior to this update, the **mkdumprd** utility was not allowed to create temporary files in the **tmpfs** file system, rendering the **kdump** service unable to start in a diskless environment. With this update, the underlying source code has been adapted to allow the use of the **tmpfs** file system, so that **kdump** is now able to start on diskless nodes as expected.

BZ#692449

Previously, running the **makedumpfile** utility with the dump level (that is, the **-d** option) set to **16** or **31** may have caused the utility to fail. This update applies a patch that addresses this issue, and **makedumpfile** now works as expected.

BZ#692685

With this update, the **mkdumprd** utility has been adapted to provide support for the **`--override-resettable`** option. This allows system administrators to start the **kdump** service on otherwise unsupported devices, such as HP Smart Array Controllers that use the **hpsa** or **cciss** driver.

BZ#693015

Prior to this update, the **kdump** crash recovery service was unable to find an LVM device identified by a *universally unique identifier* (UUID). Consequent to this, when a system crashed, **kdump** may have failed to write a core dump to such a device. This update fixes this error, and **kdump** now locates LVM devices according to their UUIDs as expected.

Enhancements

BZ#598064

After the installation of Red Hat Enterprise Linux 6, the **firstboot** application now allows users to edit the content of the **`/etc/kdump.conf`** configuration file.

BZ#632709

Support for IBM System z has been added.

BZ#672109

Previously, when the **makedumpfile** utility was used to translate a core dump file to the kdump-compressed format, it removed the ELF note section. Since this section contains potentially important information, this update adapts **makedumpfile** preserve this section in the kdump-compressed core dump files.

All users of kexec-tools are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

1.117.2. RHBA-2011:1387 — kexec-tools bug fix update

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

The kexec-tools package contains the /sbin/kexec binary and utilities that together form the user-space component of the kernel's kexec feature. The /sbin/kexec binary facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel.

Bug Fixes

BZ#719917

Previously, the mkdumprd utility failed to parse the /etc/mdadm.cof configuration file. As a consequence, mkdumprd failed to create an initial ramdisk for kdump crash recovery and the kdump service failed to start. With this update, mkdumprd has been modified so that it now parses the configuration file and builds initrd correctly. The kdump service now starts as expected.

BZ#726603

On the PowerPC 64 architecture, the kexec utiliity experienced a segmentation fault when the kdump service was started on a system containing more than 1 TB of RAM. As a result, it was not possible to capture a crash kernel on such a system. This has been fixed with this update so that kexec no

longer crashes when kdump starts on a system with greater than 1 TB of physical memory, and kdump can now works as expected.

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

1.118. krb5

1.118.1. RHSA-2011:1379 — Moderate: krb5 security update

Updated krb5 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

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

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third-party, the Key Distribution Center (KDC).

Security Fixes

CVE-2011-1527, CVE-2011-1528, CVE-2011-1529

Multiple NULL pointer dereference and assertion failure flaws were found in the MIT Kerberos KDC when it was configured to use an LDAP (Lightweight Directory Access Protocol) or Berkeley Database (Berkeley DB) back end. A remote attacker could use these flaws to crash the KDC.

Red Hat would like to thank the MIT Kerberos project for reporting the CVE-2011-1527 issue. Upstream acknowledges Andrej Ota as the original reporter of CVE-2011-1527.

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct these issues. After installing the updated packages, the krb5kdc daemon will be restarted automatically.

1.118.2. RHBA-2011:0571 — krb5 bugfix update

Updated krb5 packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

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).

Kerberos has been upgraded to version 1.9, which provides a number of bug fixes over the previous version. (BZ#642417)

Bug Fixes

BZ#595841, BZ#595842

Previously, no IPv6 suport was available for kprop, kpropd, kadmin and kadmind. This update adds IPv6 support to these utilities.

BZ#627039

Previously, the krbPwdExpiration attribute in the principal's entry would often be ignored when the realm database was stored in a directory server. This update fixes this problem and this attribute is no longer ignored.

BZ#629022

Previously, kinit with smart card login did not authenticate to the KDC correctly if the certificate on the smart card did not contain a subjectAltName extension or multiple certificates were available and krb5.conf was configured to select according to the value of the keyUsage extension in the certificates. This update continues to look for certificates with the right extension and corrects the valuation.

BZ#630587

Previously, the init script for the kpropd was not Linux Standards Base (LSB) compliant. With this update, this init script is LSB compliant.

BZ#630968

Previously, the KDC log files were not rotated by default. This update corrects this problem. Now these log files are rotated correctly.

BZ#646499

Previously, logins failed if the user had a .k5login file which did not explicitly contain the user's principal name. With this update, this check can be disabled using the "k5login_authoritative" setting in krb5.conf.

BZ#679612

Previously, GSSAPI authentication from Windows clients using cross-realm authentication failed if the client's ticket included a Privilege Attribute Certificate (PAC) with a failed signature check. Failed signature checks are now ignored.

All krb5 users are advised to upgrade to these updated packages, which fix these bugs.

1.118.3. RHBA-2011:0907 — krb5 bug fix update

Updated krb5 packages that fixes a bug is now available for Red Hat Enterprise Linux 6.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other with the help of a trusted third party, a KDC (Key Distribution Center).

Bug Fix

BZ#714866

Certain versions of the KDC software (included for example in Red Hat Enterprise Linux 2.1 and 3) reject requests, which include KDC options the software does not recognize, and do not support the "canonicalize" option. When a client was configured to use one of these versions of the KDC software, the client failed to obtain credentials for authentication to other services. This interoperability regression was introduced in the update to Red Hat Enterprise Linux 6.1. With this update, an upstream patch has been provided to fix this bug.

Users of krb5 are advised to upgrade to these updated packages, which fix this bug.

1.119. krb5-appl

1.119.1. RHSA-2011:0920 — Important: krb5-appl security update

Updated krb5-appl packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having 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 krb5-appl packages provide Kerberos-aware telnet, ftp, rcp, rsh, and rlogin clients and servers. While these have been replaced by tools such as OpenSSH in most environments, they remain in use in others.

Security Fix

CVE-2011-1526

It was found that gssftp, a Kerberos-aware FTP server, did not properly drop privileges. A remote FTP user could use this flaw to gain unauthorized read or write access to files that are owned by the root group.

Red Hat would like to thank the MIT Kerberos project for reporting this issue. Upstream acknowledges Tim Zingelman as the original reporter.

All krb5-appl users should upgrade to these updated packages, which contain a backported patch to correct this issue.

1.119.2. RHBA-2011:0687 — krb5-appl bug fix update

Updated krb5-appl packages are now available for Red Hat Enterprise Linux 6.

The krb5-appl package contains Kerberos-aware versions of telnet, ftp, rcp, rsh, and rlogin clients and servers. While these have been replaced by tools such as OpenSSH in most environments, they remain in use in others.

Bug Fix

BZ#632442

kshd, the Kerberos-aware version of rshd, unnecessarily failed if the name of the local user account being accessed was more than 16 characters long. This occurred despite the user name being accepted by klogind, the Kerberos-aware version of rlogind. In this update, kshd was modified to accept user names with the length of up to 32 characters as accepted by klogind.

Users are advised to upgrade to these updated krb5-appl packages, which resolve this issue.

1.120. ldapjdk

1.120.1. RHBA-2011:0803 — ldapjdk bug fix update

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

The Mozilla LDAP SDKs enable you to write applications which access, manage, and update the information stored in an LDAP directory.

Bug Fix

BZ#684028

When parsing an attribute definition from a directory server schema entry, the ldapjdk parser did not properly handle the ORDERING and SUBSTR matching rule specifications.

This bug was being encountered by:

1) RHDS customers using the 389-ds-console code;

-or-

2) Custom applications while using the

LDAPSchemaElement.getOptionalValues() or LDAPAttributeSchema.getValue() methods to get a string representation of an LDAP attribute that has multiple matching rule types present.

The offending method in ldapjdk was fixed so that new attributes with multiple matching rule types are created properly.

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

1.121. libarchive

1.121.1. RHSA-2011:1507 — Moderate: libarchive security update

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

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

The libarchive programming library can create and read several different streaming archive formats, including GNU tar and cpio. It can also read ISO 9660 CD-ROM images.

Security Fixes

CVE-2011-1777, **CVE-2011-1778**

Two heap-based buffer overflow flaws were discovered in libarchive. If a user were tricked into expanding a specially-crafted ISO 9660 CD-ROM image or tar archive with an application using libarchive, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

All libarchive users should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications using libarchive must be restarted for this update to take effect.

1.122. libcacard

1.122.1. RHBA-2011:0583 — libcacard bug fix and enhancement update

New libcacard packages, and an updated spice-client package that fixes number of bugs and adds various enhancements, are now available for Red Hat Enterprise Linux 6.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol

designed for virtual environments which allows users to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet. The spice-client package contains the spicec program, which renders a virtual desktop using the SPICE protocol.

The new libcacard package contains Common Access Card (CAC) emulation library.

The spice-client package has been upgraded to upstream version 0.8.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#671383)

Bug Fixes

BZ#630825, BZ#626975

When a kernel panic occurred on a guest, spice-client blinked the LED lights for the Num lock and Caps Lock keys even when it did not have keyboard focus, making it virtually impossible to type in another window. This bug has been fixed and both keys now work as expected.

BZ#628573

The X Window Server occasionally used over 80% of CPU time while the client was in full-screen mode, which caused the user's desktop session to become very unresponsive. This bug has been fixed and the undesired overhead no longer occurs.

BZ#642149

When switching to full-screen mode using the Shift+F11 shortcut, spice-client did not work properly with certain window managers such as Compiz. This bug has been fixed and the full-screen mode now works as expected in modern window managers.

BZ#644292

When running the "spicec --controller" command without having set the SPICE_XPI_SOCKET environment variable, users could experience unexpected termination caused by a segmentation fault. This bug has been fixed and spicec now exits cleanly with an error message in this particular scenario.

BZ#653535

Using the Red Hat Enterprise Virtualization Manager, when a guest connected to a virtual machine (VM) via spicec, the window received title that differed from the VM name. This bug has been fixed and the user window's title now matches the name of the VM.

BZ#655029

A watermark banner was visible during the whole session and it obstructed the user's view. This update disables the banner so that it no longer obstructs the view.

BZ#670238

When spice-client was set to use JPEG compression for images, the client sometimes terminated unexpectedly. This bug has been fixed and the spice-client now handles JPEG images properly.

BZ#670274

If the client failed verification because of a subject mismatch between the supplied host and the actual host, the error message given was too short to be useful. With this update, the error message is now sufficiently informative.

BZ#670276

The spicec program incorrectly parsed long arguments when an equal sign ("=") was used. As a result, an error message was given and the client did not start. This bug has been fixed and the client now behaves as expected.

BZ#675767

When a spice-client hotkey was set to Ctrl+Alt, users were unable to send, using Sticky-Alt, a Ctrl+Alt+key key sequence to a guest. That prevented various functionality such as switching focus to the console or setting keyboard shortcuts. This bug has been fixed and users can send the client a key sequence with Ctrl and Alt keys using Sticky-Alt even if a spice-client hotkey is set to Ctrl+Alt.

BZ#679467

Status changes of the Caps Lock and Num Lock key were not synchronized from the guest to the client. With this update a guest and a client always synchronize their status of the Caps Lock and Num Lock keys.

BZ#680763

Sometimes, spicec became stuck when exiting from full-screen mode if it received an asynchronous X Window system error. With this update, spicec now correctly calls the appropriate "_exit()" function in this rare circumstance so that spicec does not become stuck if this situation occurs.

Enhancements

BZ#644258

With an appropriate spice-server installed and a spice-agent running, users of spice-client can now copy-and-paste between the guest and the client.

BZ#545936

With this update, the following features have been added to the spice-client package to support a WAN (wide area network) environment: lossy compression for RGBA images on WAN connections, zlib compression (over GLZ) on WAN connections, an option to disable guest display effects such as animations, and an option to set guest color-depth.

BZ#675085

The spice-server and spice-client packages use common libraries in Red Hat Enterprise Linux 6.1. This renders the following packages obsolete: cairo-spice version 1.8.7.2 and earlier, ffmpeg-spice version 0.4.9-1 and earlier, pixman-spice version 0.13.3-6 and earlier, and spice-common version 0.4.2-8 and earlier. These removed and obsoleted packages are now recorded in the spice-server.spec file.

NOTE

Note that if both spice-client and spice-server are installed on a system, upgrading one of them will also cause the other to be upgraded.

BZ#641829

The spice-client package now supports Common Access Cards (CACs), allowing single sign-on and other card services such as encryption.

BZ#641831

The spice-client package now supports Red Hat Enterprise Linux Single Sign-On (SSO) functionality with properly-configured smart card readers.

Users of spice-client should upgrade to these updated packages, which fix these bugs and add these enhancements.

1.123. libcgroup

1.123.1. RHBA-2011:0577 — libcgroup bug fix and enhancement update

Updated libcgroup packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

The libcgroup packages provide tools and libraries to control and monitor control groups.

Bug Fixes

BZ#620368

With this update, the cgred and cgconfig services return proper exit codes when an error occurs.

BZ#622462

The cgconfig service was erroneously setting values of configured parameters in the reverse order as they were written in the /etc/cgconfig.conf file. With this update, the cgconfig service now correctly sets parameter values in the same order as they appear in the configuration file.

BZ#626127

The cgget command (which prints parameters of given cgroups) did not correctly display information about resource controllers due to a small buffer size. With this update, the buffer is no longer limited in size and the cgget command displays correct information.

BZ#628895

The cgcreate command changed the current working directory when creating a cgroup. The command restored the working directory to the previous location, however, some directory changes could have been refused (for example, SELinux; resulting in cryptic security denials). With this update, the cgcreate command no longer changes the current working directory and therefore no longer incurs any SELinux denials.

BZ#635984

After re-mounting a hierarchy of cgroups, the lssubsys command displayed incorrect information about the mounted hierarchies. This update fixes the faulty parsing of mounted hierarchies which are now correctly displayed.

BZ#650984

The cgred service failed to start if the cgconfig service was not running and returned the following error: "libcgroup initialization failed, 50001". With this update, a more human-readable error message is returned when the cgred service is started before the cgconfig service.

BZ#667957

The cgclassify command returned exit code 1 even if no errors occurred. With this update, exit code 0 is returned in the aforementioned case.

BZ#679698

The /etc/cgconfig.conf file could not contain parameter values with special characters such as commas. Therefore, it was not possible to set certain values for some parameters (for example, cpuset.cpus=0,2). With this update, the cgconfig.conf parser allows enclosing the parameter values inside double quotes which allow special characters to be defined inside them (for example, cpuset.cpus="0,2").

Enhancement

BZ#649195

The libcgroup package now includes the cgsnapshot tool which is used to write the current state of control groups to a configuration file.

Users are advised to upgrade to these updated libcgroup packages, which resolve these issues and add this enhancement.

1.124. libcmpiutil

1.124.1. RHEA-2011:0641 — libcmpiutil enhancement update

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

The libcmpiutil library provides an API for performing common tasks with various Common Manageability Programming Interface (CMPI) providers.

Enhancement

BZ#633332

The libcmpiutil package has been upgraded to upstream version 8.5.4, which improves performance and is a prerequisite for the new interfaces provided by the libvirt-cim package update as the package depends on the libcmpiutil library.

Users of libcmpiutil are advised to upgrade to this updated package, which adds this enhancement.

1.125. libcxgb3

1.125.1. RHBA-2011:0758 — libcxgb3 bug fix and enhancement update

Updated libcxgb3 packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

libcxgb3 is a device-specific driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio Internet Wide Area RDMA Protocol (iWARP) capable ethernet devices.

This update upgrades libcxgb3 to upstream version 7.10, which provides multiple bug fixes and enhancements over the previous version. (BZ#675025)

All users of libcxgb3 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.126. libdfp

1.126.1. RHBA-2011:0659 — libdfp bugfix update

Updated libdfp packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

The libdfp packages contain the Decimal Floating Point C Library, which is inter alia used for converting strings into decimal floating point numbers.

The libdfp packages have been upgraded to upstream version 1.0.6, which provides a number of bug fixes over the previous version. (BZ#642693)

Bug Fixes

BZ#625495

Previously, converting a string into a decimal floating point number greater than zero and less than one caused an error. During this conversion, the first decimal digit disappeared; consequently all following computations were done with wrong numbers. This bug has been fixed so that the conversion into the decimal floating point number now works as expected.

BZ#628670

Under some circumstances, libdfp encountered an issue while converting a value from a string into a decimal floating point number with the conversion command "strtod32". The "strtod64" and "strtod128" commands, which are also included in libdfp, did work correctly. The problem has been resolved so that the conversion now proceeds properly.

BZ#673222

Previously, there were several testsuite failures encountered when building the libdfp packages for the IBM S/390 architecture. These testsuite failures have been corrected with this update and thus no longer occur.

All users requiring libdfp should upgrade to these updated packages, which fix these bugs.

1.127. libgcrypt

1.127.1. RHBA-2011:0726 — libgcrypt bug fix update

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

The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.

Bug Fixes

BZ#576549

Previously, the build time test did not support FIPS (Federal Information Processing Standard) mode and failed in this mode. This update modifies the test so that it passes successfully on machines set to use FIPS mode.

BZ#669084

In FIPS mode, libgcrypt used the /dev/random device as the source for the RNG (Random Number Generator) seed. This caused the RNG initialization in FIPS mode to take several minutes. With this update, libgcrypt uses the /dev/urandom device for the RNG seed and RNG initialization no longer causes any delays.

All users of libgcrypt are advised to upgrade to this updated package, which resolves these issues.

1.127.2. RHEA-2011:0846 — libgcrypt enhancement update

An updated libgcrypt package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.

Enhancement

BZ#709059

With this update, the libgcrypt API for the DSA algorithm has been enhanced to allow for presetting the prime (P) and the subprime (Q) parameters when generating the base (G) parameter. This is necessary for the algorithm correctness validation according to the FIPS-186-3 standard.

All users of libgcrypt are advised to upgrade to this updated package, which adds this enhancement.

1.127.3. RHEA-2011:0515 — libgcrypt enhancement update

An updated libgcrypt package that introduces a feature enhancement is now available for Red Hat Enterprise Linux 6.

The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.

Enhancement

BZ#703490

In FIPS mode, libgcrypt can now use a configurable source of RNG (Random Number Generator) seed. On systems with sufficient amount of entropy gathered from the kernel entropy sources or systems with hardware RNGs, the system administrator can add the "/etc/gcrypt/rngseed" symbolic link pointing to the "/dev/random" device node or a hardware RNG device. This symbolic link will be then opened and read by the libgcrypt library to initialize its RNG.

All users of libgcrypt are advised to upgrade to this updated package, which adds this enhancement.

1.128. libgssglue

1.128.1. RHBA-2011:0789 — libgssglue bug fix update

Updated libgssglue packages that fix two bugs are now available.

The libgssglue packages provide a library required by programs in the rpcbind package. This library exports a GSSAPI interface that calls GSSAPI routines in other libraries.

Bug Fixes

BZ#558941

Previously, the libgssglue library files were placed in the "/usr/lib/" or "/usr/lib64/" directory, depending on the architecture. As the library is required by rpcbind which is installed in "/sbin/", this update moves the libgssglue library files to "/lib/" or "/lib64/".

BZ#681660

Previously, it was not possible to install both the 32-bit and 64-bit -devel packages simultaneously. This update resolves this multi-arch conflict.

All libgssglue and rpcbind users should install these updated packages, which address these issues.

1.129. libguestfs

1.129.1. RHSA-2011:0586 — Low: libguestfs security, bug fix, and enhancement update

libguestfs is a library for accessing and modifying guest disk images.

Updated libguestfs packages that fix one security issue and several bugs, and add a number of enhancements, are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are linked to from the security descriptions below.

Security Fix
libguestfs relied on the format auto-detection in QEMU rather than allowing the guest image file format to be specified. A privileged guest user could potentially use this flaw to read arbitrary files on the host that were accessible to the user on that host by running a program that utilized the libguestfs library. (CVE-2010-3851)

Libguestfs has been rebased to upstream version 1.7.17, which includes the following bug fixes and enhancement (BZ#613593):

BZ#600144

The **guestfish** **`mkmountpoint`** and **`umount-all`** commands are considered incompatible. Mount points created with the **`mkmountpoint`** command become invalid after the **`umount-all`** command is used. This is now documented in the **guestfish** man page. Customers should note that it is possible to safely unmount devices that were mounted with **`mkmountpoint`** by using the **`umount`** command.

BZ#612308

The **`-net`** and **`vlan=...`** options in the qemu package are deprecated. To avoid relying on these deprecated options, libguestfs now uses the **`-netdev`** option instead.

BZ#615223

The **guestfish** **`vfs-type`** command could not determine the type of a file system newly created by **guestfish**. This occurred because the **`vfs-type`** command tried to read the type from a cache file (**`blkid.c`**) that had not yet been updated. The cache file is now deleted between file system creation and attempting to read the file system type, resulting in updated file system information for **`vfs-type`** to read.

BZ#617440

If the **`$HOME`** variable was not set, **guestfish** did not expand a path containing ~ (tilde) into a path to the user's home directory. Guestfish now examines the current user's **`passwd`** file for the location of the user's home directory so that a path containing ~ can be expanded correctly.

Additionally, an off-by-one error was discovered in the same path-expansion algorithm. This error could potentially cause a crash. The off-by-one error has been corrected so that this crash is no longer possible.

BZ#627468

The **virt-inspector** and **virt-v2v** tools did not work for Windows guests if an additional package, libguestfs-winsupport, was not installed. The error message did not explicitly state that this missing package could be responsible for the error. An additional note has been added to make the error output more useful when attempting to use these tools with Windows guests.

BZ#627832

Some **guestfish** commands print integer results. In some cases, namely for file permissions, the natural radix for these results is octal. Instead, **guestfish** returned decimal integer results for commands such as **umask**. This has been corrected, and **guestfish** commands that return integers now return them in the natural radix for that number.

BZ#627833

The **get-e2uuid** command retrieved file system UUIDs via **tune2fs -l**. This failed on journaling block devices (JBDs) and other devices that were not second, third or fourth extended file systems (ext2, ext3 or ext4). **get-e2uuid** has been reimplemented so that it retrieves UUIDs via **blkid** instead of **tune2fs -l**, resolving this issue. However, since the **get-e2uuid** command has been deprecated, customers are advised to retrieve UUIDs with the **vfs-uuid** command instead.

BZ#633174

Some **guestfish** commands would hang when applied to non-regular files. This had some security implications in that a guest could replace regular configuration files with, for example, character devices, and cause **virt-inspector** and other programs to hang. **guestfish** commands have been modified and can now handle non-regular files.

Additionally, **virt-inspector** has been rewritten as **virt-inspector2**, which is both more powerful, and more careful about untrusted files from the guest.

BZ#639601

libguestfs documentation did not specify that special characters should be surrounded by quotes or otherwise "escaped" when used with the **virt-ls** at the command line. The following has been added to the libguestfs documentation:

> Libvirt guest names can contain arbitrary characters, some of which have meaning to the shell such as # and space. You may need to quote or escape these characters on the command line. See the shell manual page **sh(1)** for details.

BZ#639602

libguestfs documentation did not specify that special characters should be surrounded by quotes or otherwise "escaped" when used with the **virt-list-filesystems** at the command line. The following has been added to the libguestfs documentation:

> Libvirt guest names can contain arbitrary characters, some of which have meaning to the shell such as # and space. You may need to quote or escape these characters on the command line. See the shell manual page **sh(1)** for details.

BZ#657472

The **guestfish checksum** command contained a file descriptor that was not closed properly in an error path. If the **checksum** command resulted in an error, this would later prevent the file system from being unmounted with either **umount** or **umount-all**. The file descriptor is now closed

properly on the error path, so an error in **checksum** no longer causes problems unmounting file systems.

BZ#657502

The virt-inspector package had an unnecessary dependency on the perl-String-ShellQuote package. This superfluous dependency has been removed.

Note that this bug was reported and corrected during development. It was not seen in production systems in the field.

BZ#666577

If the **/etc/fstab** of a guest machine contained a reference to a floppy disk (**/dev/fd0**), both **virt-inspector** and **virt-v2v** printed the following harmless warning during inspection or conversion:

```
unknown filesystem /dev/fd0
```

This warning has been suppressed to avoid confusion, and should no longer appear even if the guest machine refers to floppy disks in **/etc/fstab**.

BZ#666579

If the **/etc/fstab** of a guest machine contained a reference to a CD-ROM drive (**/dev/hdc**), both **virt-inspector** and **virt-v2v** printed the following harmless warning during inspection or conversion:

```
unknown filesystem /dev/hdc
```

This warning has been suppressed to avoid confusion, and should no longer appear even if the guest machine refers to CD-ROM drives in **/etc/fstab**.

BZ#668115

The **virt-filesystems** command failed when used against a guest which had a missing or corrupt file system label. This command has been updated to handle guest file systems with missing or corrupt file system labels.

Note that this bug was reported and corrected during development. It was not seen in production systems in the field.

BZ#668611

When a device in **/etc/fstab** did not exist, the **guestfish -i** command failed with a "No such file or directory" error. In the event of missing devices, **guestfish** now completes, and reports that some file systems could not be mounted.

Note that this bug was reported and corrected during development. It was not seen in production systems in the field.

BZ#669840

The febootstrap package contained tools required to both build and run libguestfs. This package has now been split into two parts: febootstrap and febootstrap-supermin-helper. febootstrap now contains only tools used to create supermin appliances. A new package, febootstrap-supermin-helper, is a helper tool used to rebuild supermin appliances on the fly. libguestfs now depends only on the smaller febootstrap-supermin-helper package. Fresh libguestfs installations to Red Hat Enterprise Linux 6.1 now require less space because of this smaller dependency.

BZ#673477

Separating libguestfs trace output from debug output was difficult. A string (**`libguestfs: trace:`**) is now added to the beginning of each line of the trace output so that it can be easily distinguished and filtered out of logs with the **`grep`** command or similar.

BZ#673721

The **virt-make-fs** man page referred to the non-existent tool **`virt-make-resize`**. This reference should have been to the **virt-make-fs** tool. The man page has been corrected.

BZ#676788

The **guestfish** **`set-trace`** command was not prepared to handle all possible error conditions. This resulted in a segmentation fault when attempting to handle several conditions. The command now handles trace errors separately, so the segmentation fault no longer occurs.

Note that this bug was reported and corrected during development. It was not seen in production systems in the field.

BZ#691724

If the **`/etc/fstab`** of a guest machine contained a reference to a virtio disk (**`/dev/vda1`**), **virt-inspector** printed a warning and ignored the virtio disk. The warning has been suppressed, and virtio disks are now recognized by **virt-inspector**.

BZ#695138

A superfluous dependency on the gfs2-utils package has been removed.

All libguestfs users are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

1.130. libguestfs-winsupport

1.130.1. RHEA-2011:0792 — libguestfs-winsupport enhancement update

An enhanced libguestfs-winsupport package is now available for Red Hat Enterprise Linux 6.

The libguestfs-winsupport package adds support for Windows guests to libguestfs, a set of tools and libraries allowing users to access and modify virtual machine (VM) disk images.

Bug Fix

BZ#691555

The debuginfo subpackage contained no data and has been removed.

Enhancement

BZ#670299

The libguest-winsupport package depended on the entire febootstrap package. Since the febootstrap package was split into the febootstrap package and febootstrap-supermin-helper packages, libguest-winsupport now depends only on the febootstrap-supermin-helper package, which contains the runtime part of the original febootstrap package.

Users of libguestfs-winsupport are advised to upgrade to this updated package, which adds this enhancement and fixes this bug.

1.131. libhbalinux

1.131.1. RHBA-2011:0799 — libhbalinux bug fix update

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

The libhbalinux library is a vendor library utilized by fcoe-utils. The libhbaapi library provides programmatic access to the libhbalinux library. This library can retrieve adapter information with the assistance of libpciaaccess.

Bug Fixes

BZ#690014

Creating an FCoE (Fibre Channel over Ethernet) interface, by executing the "fceoadm -c [interface]" command, and shortly after the creation executing the "fcoeadm -i" command (which displays information about FCoE instances), resulted in a segmentation fault due to a NULL pointer dereference. This update fixes this issue and a segmentation fault no longer occurs in the aforementioned case.

BZ

After upgrading the libhbalinux package, the "fcoeadm -i" command (which shows information about FCoE instances) printed an error message. With this update, the "fcoeadm -i" command has been fixed, and no longer returns an error message

All users of libhbalinux are advised to upgrade to this updated package, which resolves these issues.

1.132. libica

1.132.1. RHBA-2011:0676 — libica bug fix update

Updated libica packages that fix various bugs are now available.

A library of functions and utilities for accessing ICA hardware crypto on IBM zSeries.

Bug Fixes

BZ#640035

Previously, when the libica library ran in 31-bit mode, the STCK buffer length was smaller than required, which caused corrupted memory and application crashes. This is now fixed to ensure that the libica library allocates an appropriately sized STCK buffer in 31-bit mode to prevent corrupted memory and application crashes.

BZ#665401

Previously, a SIGILL handler wrapped all cryptographic operations and caught crashes caused by invalid CPU instructions. This SIGILL handler prevented crashes but caused significant performance regression in the system. This is now fixed so that the CPU correctly reports the availability of individual cryptographics algorithms, therefore the SIGILL wrappers are removed.

BZ#624005

The libica testsuite failed for libica_keygen_test and libica_sha1_test. The test failed for libica_sha1_test because "return to zero" was missing for the old_api_sha_test() function. The libica_keygen_test test failed because the openSSL powered RSA exponent only handles the values 3 or 65537 and libica_keygen_test provided a default random value. This is now fixed so that libica_sha1_test's old_api_sha_test includes "return to zero" and libica_keygen_test runs with parameters, "libica_keygen_test <keylength> <3|65537>". Due to this, the libica testsuite no longer fails for libica_keygen_test and libica_sha1_test.

Users are advised to upgrade to these updated packages, which resolves these issues.

1.133. libnl

1.133.1. RHBA-2011:0795 — libnl bug fix update

An updated libnl package that fixes various bugs is now available.

This package contains a convenience library to simplify using the Linux kernel's netlink sockets interface for network manipulation.

Bug Fixes

BZ#620345

When a domain started under libvirt, a memory leak was triggered from the libnl library because libnl continued to use memory no longer in use. Memory leaks in libnl are now fixed and libnl releases memory after it completes usage.

BZ#677725, BZ#677724

The port allocation/de-allocation was not safe in multi-threaded applications and the logic was incorrect, which resulted in some applications and other libraries being unable to initialize libnl. Port allocation/de-allocation and logic is now fixed, and libnl can now be initialized. ()

All libnl users should upgrade to this updated package, which resolves these issues.

1.134. libpciaccess

1.134.1. RHBA-2011:0806 — libpciaccess bug fix update

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

libpciaccess is a low level system library used to access PCI devices. It provides this functionality for X.Org and virtualization layers.

Bug Fixes

BZ#675756

If pci_system_init/pci_system_cleanup was run twice (or more) in a row within the one process, a double close() could occur on the config_fd variable. This caused an error, as the FD associated with nullfd was closed by the second pci_get_strings() call. That was because the pci_device_linux_sysfs_destroy() failed to re-initialize the global 'config_fd' variable to -1 after closing it. This patch adds a line to set config_fd to -1 after the closure, fixing the issue.

BZ#675758

When the pci_system_init() function opened the /proc/mtrr file and saved its file descriptor, then pci_system_cleanup() would fail to close the file descriptor. This resulted in a leak of the FD. With this update, added to the above bug's patch, the file descriptor is closed as expected.

All users of libpciaccess are advised to upgrade to these updated packages which resolve these issues.

1.135. libpng

1.135.1. RHSA-2011:1105 — Moderate: libpng security update

Updated libpng packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

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

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Security Fixes

CVE-2011-2690

A buffer overflow flaw was found in the way libpng processed certain PNG image files. An attacker could create a specially-crafted PNG image that, when opened, could cause an application using libpng to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-2501

Note: The application behavior required to exploit CVE-2011-2690 is rarely used. No application shipped with Red Hat Enterprise Linux behaves this way, for example.

An out-of-bounds memory read flaw was found in the way libpng processed certain PNG image files. An attacker could create a specially-crafted PNG image that, when opened, could cause an application using libpng to crash.

CVE-2011-2692

An uninitialized memory read issue was found in the way libpng processed certain PNG images that use the Physical Scale (sCAL) extension. An attacker could create a specially-crafted PNG image that, when opened, could cause an application using libpng to crash.

Users of libpng should upgrade to these updated packages, which upgrade libpng to version 1.2.46 to correct these issues. All running applications using libpng must be restarted for the update to take effect.

1.136. librsvg2

1.136.1. RHSA-2011:1289 — Moderate: librsvg2 security update

Updated librsvg2 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 librsvg2 packages provide an SVG (Scalable Vector Graphics) library based on libart.

Security Fix

CVE-2011-3146

A flaw was found in the way librsvg2 parsed certain SVG files. An attacker could create a specially-crafted SVG file that, when opened, would cause applications that use librsvg2 (such as Eye of GNOME) to crash or, potentially, execute arbitrary code.

Red Hat would like to thank the Ubuntu Security Team for reporting this issue. The Ubuntu Security Team acknowledges Sauli Pahlman as the original reporter.

All librsvg2 users should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications that use librsvg2 must be restarted for this update to take effect.

1.137. libselinux

1.137.1. RHBA-2011:0751 — libselinux bug fix update

Updated libselinux packages that fix various bugs are now available.

libselinux is the core library of an SELinux system. It provides an API for SELinux applications to get and set process and file security contexts and to obtain security policy decisions. It is required for any applications that use the SELinux API and used by all applications that are SELinux-aware.

Bug Fixes

BZ#658571

libselinux used __thread variables to store malloc() data in order to minimize computation. Destructors cannot be associated with __thread variables, so malloc() data stored in a __thread void* variable could potentially cause memory leaks upon thread exit. For example, repeatedly starting and stopping domains with libvirt could trigger out-of-memory exceptions, since libvirt starts one thread per domain, and each thread uses libselinux calls such as fgetfilecon. libselinux has been updated to be thread-safe, preventing these potential memory leaks.

BZ#693600

An update to libselinux added global destructors, which deleted thread-specific keys without checking that they had been initialized. Since the keys were not always initialized with the pthread_key_create() method and their default value was 0, it was possible that key 0 would be removed by these destructors. This resulted in segmentation faults in programs using active threads whose keys were removed, specifically in OpenJDK. Keys now receive a default value of -1, protecting uninitialized keys from attempts by global destructor to delete them. Note that this issue was discovered and corrected during development, and was not seen in production systems in the field.

BZ#680887

An update to libselinux caused a segmentation fault to appear in the multi-threaded pam_chauthtok() test program. If a shared library attempted to call pthread_key_create(), the associated destructors

were registered with that library. The segmentation fault occurred when pthread_key_delete() was called, if that library was dereferenced with dlclose() before the destructors were removed with pthread_key_delete(). This issue has now been corrected. Note: this issue was discovered and corrected during development, and was not seen in production systems in the field.

All users of libselinux are advised to upgrade to these updated packages, which resolve these issues.

1.138. libsndfile

1.138.1. RHSA-2011:1084 — Moderate: libsndfile security update

Updated libsndfile 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 libsndfile packages provide a library for reading and writing sound files.

Security Fix

CVE-2011-2696

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way the libsndfile library processed certain Ensoniq PARIS Audio Format (PAF) audio files. An attacker could create a specially-crafted PAF file that, when opened, could cause an application using libsndfile to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Users of libsndfile are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libsndfile must be restarted for the update to take effect.

1.139. libsoup

1.139.1. RHSA-2011:1102 — Moderate: libsoup security update

Updated libsoup 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.

libsoup is an HTTP client/library implementation for GNOME.

Security Fix

CVE-2011-2524

A directory traversal flaw was found in libsoup's SoupServer. If an application used SoupServer to implement an HTTP service, a remote attacker who is able to connect to that service could use this flaw to access any local files accessible to that application via a specially-crafted request.

All users of libsoup should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running applications using libsoup's SoupServer must be restarted for the update to take effect.

1.140. libssh2

1.140.1. RHBA-2011:1373 — libssh2 bug fix update

An updated libssh2 package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The libssh2 package provides a library that implements the SSH2 protocol.

Bug Fix

BZ#743511

Prior to this update, libssh2 package leaked memory and terminated unexpectedly in certain situations. This update modifies libssh2 so that no more memory leaks occur and now libssh2 works as expected.

Note, that all running applications using libssh2 have to be restarted for the update to take an effect.

All users of libssh2 are advised to upgrade to this updated package, which fixes this bug.

1.141. libtdb

1.141.1. RHBA-2011:0808 — libtdb bug fix update

Updated libtdb packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

The libtdb package contains a library that implements a trivial database.

Bug Fix

BZ#692251

When processing very large database updates, occasionally, tdb incorrectly allocated unnecessarily large amounts of memory. As a result, an OOM (Out Of Memory) situation occurred. This was caused by libtdb calling the tdb_expand() function to increase its size by creating space to store an extra hundred records of the size of the largest record it currently has. With this update, this behavior has been removed and tdb no longer allocates unnecessarily large amounts of memory.

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

1.142. libtirpc

1.142.1. RHBA-2011:0747 — libtirpc bug fix update

An updated libtirpc package that fixes various bugs is now available.

The libtirpc package contains SunLib's implementation of transport independent RPC (TI-RPC) documentation. This includes a library required by programs in the nfs-utils and rpcbind packages.

Bug Fixes

BZ#558937

Binaries in the nfs-utils package located in /sbin relied on shared libraries located in /usr. This has been fixed so that nfs-utils binaries installed in /sbin no longer rely on shared libraries in /usr/lib.

BZ#628682

Previously certain files were under SISSL license. These files are now under the BSD license and are marked with the "Copyright (c) 2010, Oracle America, Inc." license text.

BZ#676234

In a multi-homed NFS server with two IP addresses on the same subnet, mount operations sent to one IP address would result in a reply from the other IP address. This is now fixed to ensure that a mount request to one IP address elicits a response from the same IP address.

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

1.143. libvirt

1.143.1. RHSA-2011:1197 — Moderate: libvirt security and bug fix update

Updated libvirt packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having 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-2011-2511

An integer overflow flaw was found in libvirtd's RPC call handling. An attacker able to establish read-only connections to libvirtd could trigger this flaw by calling virDomainGetVcpus() with specially-crafted parameters, causing libvirtd to crash.

Bug Fixes

BZ

Previously, when the "virsh vol-create-from" command was run on an LVM (Logical Volume Manager) storage pool, performance of the command was very low and the operation consumed an excessive amount of time. This bug has been fixed in the virStorageVolCreateXMLFrom() function, and the performance problem of the command no longer occurs.

BZ#726617

Due to a regression, libvirt used undocumented command line options, instead of the recommended ones. Consequently, the qemu-img utility used an invalid argument while creating an encrypted volume, and the process eventually failed. With this update, the bug in the backing format of the storage back end has been fixed, and encrypted volumes can now be created as expected.

BZ#728516

Due to a bug in the qemuAuditDisk() function, hot unplug failures were never audited, and a hot unplug success was audited as a failure. This bug has been fixed, and auditing of disk hot unplug operations now works as expected.

BZ#728546

Previously, when a debug process was being activated, the act of preparing a debug message ended up with dereferencing a UUID (universally unique identifier) prior to the NULL argument check. Consequently, an API running the debug process sometimes terminated with a segmentation fault. With this update, a patch has been provided to address this issue, and the crashes no longer occur in the described scenario.

BZ

* The libvirt library uses the "boot=on" option to mark which disk is bootable but it only uses that option if Qemu advertises its support. The qemu-kvm utility in Red Hat Enterprise Linux 6.1 removed support for that option and libvirt could not use it. As a consequence, when an IDE disk was added as the second storage with a virtio disk being set up as the first one by default, the operating system tried to boot from the IDE disk rather than the virtio disk and either failed to boot with the "No bootable disk" error message returned, or the system booted whatever operating system was on the IDE disk. With this update, the boot configuration is translated into bootindex, which provides control over which device is used for booting a guest operating system, thus fixing this bug.

All users of libvirt are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, libvirtd must be restarted ("service libvirtd restart") for this update to take effect.

1.143.2. RHSA-2011:0596 — libvirt bug fix and enhancement update

Updated libvirt packages that upgrade the **libvirt** library to upstream version 0.8.7, fix a number of bugs, and add various enhancements and new features 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.

These updated packages upgrade the libvirt library for Red Hat Enterprise Linux 6 to upstream version 0.8.7, which contains many enhancements and bug fixes over the previous version. This section contains detailed information about a subset of bug fixes and enhancements that are likely to affect customers only. For a short summary of all changes see the **CHANGELOG** file installed to **/usr/share/doc/libvirt-0.8.7** when the updated package is installed.

Bug Fixes

BZ#515692

Guests were not required to honour the **virDomainSetMemory()** setting, making it impossible to set a hard limit on guest memory consumption. New **virDomainGetMemoryParameters** and **virDomainSetMemoryParameters** methods have been introduced to allow users to fine-tune and enforce memory limits.

BZ#561935

Live migration of a guest could take an exceptionally long time to converge to the switchover point if the guest was very busy. Migration is more likely to complete if a guest's **downtime** setting is increased. However, libvirt was sending an incorrectly formatted request to increase the **downtime**

setting of a guest. This update corrects the format of this request to assist in live migration completion.

BZ#672226

Using SASL authentication with a single libvirt connection for multiple threads could result in libvirt hanging while waiting for a response from the libvirt daemon. SASL decoding has been fixed such that clients do not wait for further data while already decoded SASL data remains unprocessed, so libvirt no longer hangs in this situation.

BZ#688774

libvirt was not careful about object locking rules when managing KVM guests, which resulted in a number of unexpected actions. If a guest shut down without notice, libvirt could crash or loop indefinitely. Locking code in libvirt has been improved to avoid accessing data outside locks, and to avoid deadlocks when multiple threads are interacting with the same domain, so libvirt no longer hangs or crashes when a guest shuts down.

BZ#677729

The port allocation/de-allocation of the libnl library, which is used by libvirt for macvtap (for example, vepa and vnlink) interfaces, was not threadsafe and the logic was incorrect. This resulted in a failure to initialize libnl, and a subsequent failure of the associated libvirt functionality. In particular, the first guest vepa interface started on a host would work, but all subsequent vepa interfaces would fail. Port allocation/de-allocation and logic is now fixed in libnl, and the failures in libvirt no longer occur.

BZ#687551

In previous releases, libvirt set a maximum lease limit for DHCP leases on each virtual network according to the number of addresses available on that network. However, all networks shared the same lease file, so the maximum lease limit was reached long before all networks had given out all of their addresses. This meant that some guests were unable to obtain IP addresses. With this release of libvirt, each virtual network uses its own lease file, so there is sufficient space for all configured addresses to be allocated.

BZ#691514

When creating virtual machines via remote protocol, the client hung because the list of remote procedure calls to execute was not traversed correctly. Traversal has been corrected so that creating virtual machines remotely no longer causes libvirt to hang.

BZ#692998

libvirt removed the managed state file (created by **`virsh managedsave dom`**) even if it failed to restore and start the domain using that file. This caused data loss. The managed state file is now removed only if the restore operation succeeds.

BZ#638285

During migration, an application could query block information on the virtual guest being migrated. This resulted in a race condition that crashed libvirt. libvirt now verifies that a guest exists before attempting to start monitoring operations.

BZ#656795

Memory buffer was not freed properly on domain startup and shutdown, which led to a memory leak that increased each time the domain was started or shut down. This update removes this memory leak.

BZ#660706

The **%post** script (part of the libvirt-client package) started the **libvirt-guests** service even when the service was explicitly turned off. The **libvirt-guests** service is no longer started when explicitly turned off.

BZ#659310

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#653293

When running **virsh vcpuinfo** or setting up virtual CPU pinning on a host machine that used NUMA, **virsh vcpuinfo** showed the incorrect number of virtual CPUs. Virtual CPU pinning could also fail because libvirt reported an incorrect number of CPU sockets per NUMA node. Virtual CPUs are now counted correctly.

BZ#660194

An off-by-one error in a clock variable caused a virtual guest to show incorrect date and time information. This update corrects this error so that date and time information is correctly displayed.

BZ#649523

A specification file bug caused permissions on the **/var/lib/libvirt** directory to change when a system was upgraded. With this update, correct permissions are assigned to the aforementioned directory.

BZ#658657

libvirt used a non-thread friendly SELinux API (matchpathcon) to get the default security context for a specified path. This led to a memory leak upon domain startup and shutdown. libvirt now uses improved SELinux APIs, so this memory leak no longer occurs.

BZ#646895

Device boot order could not be set more explicitly than Network, Disk, CD ROM, or Floppy. This meant that users could not select the exact boot device that they wished to use. A per-device **<boot>** element has been introduced, which can be used to specify the exact order of boot devices.

BZ#609463

The MAC address of libvirt's bridges could change over time depending on which guests were currently running and connected. This caused problems in some Windows guests, which assumed that the changed MAC address indicated a new network connection, and automatically launched a configuration wizard. libvirt now creates a dummy tap device with a guaranteed lowest MAC address that will not change. This address is stored as part of network configuration so that it will persist across host reboots.

BZ#611793

If the configuration for a virtual network only contained static address definitions, dnsmasq (the DHCP server used by libvirt) was started incorrectly and would not respond to any DHCP requests. Any guests with MAC address/IP address pairs listed in static address definitions were then unable to acquire their IP addresses. libvirt now starts up **dnsmasq** with the correct options so that these statically configured addresses are properly served to the guests.

BZ#639587

The **virsh freecell** command could be run with an invalid (non-integer) argument without error, and the free memory for node 0 would still be printed. The validity of the argument is now checked, and an error message is now printed when an invalid value is detected.

BZ#671050

If the **virsh detach-interface** command was used on a domain with multiple NICs, but a particular MAC address was not specified with **--mac**, virsh detached the first interface without error. The **--mac** option is now required where a domain has multiple NICs, and an appropriate error message has been added.

BZ#627143

If the user did not specify a disk driver when hot-plugging a disk with **virsh attach-disk**, virsh set **phy** as the driver value by default. Because this value is not supported everywhere, the disk did not persist over domain shutdown, and could prevent domain startup. This update corrects virsh behavior such that the driver value is not set if it is not provided by the user.

BZ#667091

libvirt incorrectly identified the virtual IB700 device (an ISA device) as a PCI device, resulting in the device being misconfigured, and preventing the virtual machine from booting until the virtual IB700 device was removed. libvirt now identifies the IB700 device correctly.

BZ#605660

Invalid **setvcpus** commands resulted in unknown errors. More useful error messages have been added to this command.

BZ#676374

A typographical error in source code that parsed and wrote SPICE **auth** data caused unrelated data to be overwritten, which caused a crash in libvirt. The error has been corrected, and **auth** can now be set without issue.

BZ#696660

The string containing the name of libvirt's "dummy" tap interface was freed before network startup was guaranteed. This caused a segmentation fault if a problem occurred while setting the **forward-delay** or **stp-enable** parameters. The string is no longer freed prematurely, and in the event of a problem with these parameters, users receive a specific error message.

BZ#689001

When a problem occurred while starting up a guest that used direct interfaces, an uninformative error message ("unspecified error") was printed to the log. These failures now have specific, more informative log messages.

BZ#611822

When the certificate used for TLS authentication was rejected, libvirt displayed a log message containing a command that had misleading output (**openssl x509 -in clientcert.pem -text**). This command has been replaced with the following command, which gives more helpful, accurate output:

```
certtool -i --infile /etc/pki/libvirt/clientcert.pem
```

Enhancements

BZ#586124

The virtual networks created and used by libvirt for virtual guest connectivity were previously limited to only IPv4 connectivity; IPv6 traffic was explicitly disallowed. Full IPv6 connectivity is now supported on libvirt's virtual networks, including autoconf address/route discovery and a DNS server listening on an IPv6 address on the network. Note, however, that because autoconf is supported, there is no support for DHCPv6.

BZ#656845

libvirt could not determine whether a domain had crashed or been correctly shut down. This update adds recognition of the SHUTDOWN event sent by qemu when a server is shut down correctly. If this event is not received, the domain is now declared to have crashed.

BZ#653530

An **`--all`** option has been added to the **`virsh freecell`** command to allow the command to iterate across all nodes instead of forcing users to run the command manually on each node. **`virsh freecell --all`** will list the free memory on all available nodes.

BZ#635419

Users can now disable memory merging (KSM) on guest machines. Note however that this requires support for the underlying qemu-kvm **`-redhat-disable-KSM`** flag.

BZ#641187

The **`virsh`** documentation has been updated to clarify usage of the **`cpu_shares`** parameter.

BZ#639603

The **`virsh`** documentation has been updated to remove references to the deprecated **`virt-mem`** command.

BZ#605660

The **`virsh`** documentation for the **`setvcpus`**, **`setmem`**, and **`setmaxmem`** sub-commands has been updated to correct and expand the information available for these sub-commands.

BZ#595350

A man page is now available for **`libvirtd`**. Access it with the **`man libvirtd`** command.

All users of libvirt are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

1.143.3. RHBA-2012:0685 — libvirt bug fix update

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

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems.

Bug Fix

BZ#816980

An application using the libvirt shared library could terminate unexpectedly with a segmentation fault when the application tried to unload the library using the dlclose() function. This could happen for example when shutting down the tog-pegasus utility while the libvirt-cim provider was in use. This update modifies linking properties of the library so that the library now prevents itself from being unloaded from memory. Applications using the libvirt shared library no longer crash in the described scenario.

All users of libvirt are advised to upgrade to these updated packages, which fix this bug. After installing these updated packages, libvirtd must be restarted. Use the "service libvirtd restart" command for this update to take effect.

1.143.4. RHBA-2011:1431 — libvirt bug fix update

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

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems. The library provides the libvirtd daemon, which is required for virtualization management of KVM and LXC.

Bug Fixes

BZ#743557

Due to a programming error in the initialization code of the libvirtd daemon, the QEMU driver could have failed to find the user or group ID of the qemu application on the system. As a result, libvirtd failed to start. With this update, the error has been corrected and libvirtd now works as expected.

BZ#747358

If the QEMU driver failed to update information about currently allocated memory, installing a new virtual machine could have failed with the following error message:

ERROR cannot send monitor command '{"execute":"query-balloon"}': Connection reset by peer

With this update, the driver has been modified to not consider this behavior as fatal. Installation now proceeds and finishes as expected.

All users of libvirt are advised to upgrade to these updated packages, which fix this bug. After installing these updated packages, libvirtd must be restarted. Use the "service libvirtd restart" command for this update to take effect.

1.144. libvirt-cim

1.144.1. RHEA-2011:0648 — libvirt-cim enhancement update

An enhanced libvirt-cim package is now available for Red Hat Enterprise Linux 6.

The libvirt-cim package contains a Common Information Model (CIM) provider based on Common Manageability Programming Interface (CMPI). It supports most libvirt virtualization features and allows management of multiple libvirt-based platforms.

Enhancements

BZ#633331

Previously, the libvirt-cim migration indications did not contain any UUID (universally unique identifier) values. This update adds the UUID values to migration indications and improves the ability of the management software to track migrated virtual machines.

BZ#633336

Previously, Virtual Ethernet Port Aggregator (VEPA) and VSI (Virtual Station Interface) networking capabilities were not supported. This update provides support for both VEPA and VSI.

All libvirt-cim users are advised to upgrade to this updated package, which adds these enhancements.

1.145. libvirt-java

1.145.1. RHBA-2011:0761 — libvirt-java bug fix and enhancement update

Updated libvirt-java packages that provide a new API, fix several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libvirt-java package provides a base framework to use libvirt, which is the virtualization API to manage and interact with the virtualization capabilities.

The libvirt-java package has been upgraded to upstream version 0.4.7, which provides a new API, improved error-handling, and enhancements over the previous version. (BZ#675044)

Users are advised to upgrade to these updated libvirt-java packages, which resolve these issues and add these enhancements.

1.146. libvirt-qpid

1.146.1. RHBA-2011:0762 — libvirt-qpid bug fix update

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

The libvirt-qpid package provides an interface with libvirt using the qpid modeling framework (QMF), which utilizes the Advanced Message Queuing Protocol (AMQP), an open standard application layer protocol providing reliable transport of messages.

Bug Fix

BZ#618876

Previously, libvirt-qpid did not correctly connect to qpid due to an authentication conflict. This update rebuilds libvirt-qpid to match the qpid-cpp package. Now, libvirt-qpid runs as expected.

Users of libvirt-qpid are advised to upgrade to this updated package, which fixes this bug.

1.147. libvpd

1.147.1. RHEA-2011:0548 — libvpd enhancement update

An updated libvpd package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The libvpd package contains the classes that are used to access Vital Product Data (VPD) created by vpdupdate in the lsvpd package.

Enhancement

BZ#632738

This update provides the latest API by which external serviceability and diagnostics tools can access VPD, consisting of hardware present on a system, the characteristics of that hardware, or hardware state.

Users of libvpd are advised to install this package, which adds this enhancement.

1.148. libXfont

1.148.1. RHSA-2011:1154 — Important: libXfont security update

Updated libXfont 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 libXfont packages provide the X.Org libXfont runtime library. X.Org is an open source implementation of the X Window System.

Security Fix

CVE-2011-2895

A buffer overflow flaw was found in the way the libXfont library, used by the X.Org server, handled malformed font files compressed using UNIX compress. A malicious, local user could exploit this issue to potentially execute arbitrary code with the privileges of the X.Org server.

Users of libXfont should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running X.Org server instances must be restarted for the update to take effect.

1.149. lldpad

1.149.1. RHBA-2011:0520 — lldpad bug fix and enhancement update

An updated lldpad package that fixes multiple bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The lldpad package provides the Linux user space daemon and configuration tool for Intel's Link Layer Discovery Protocol (LLDP) agent with Enhanced Ethernet support.

Bug Fixes

BZ#631587

Previously, lldpad did not initiate a Data Center Bridging Exchange (DCBX) negotiation if a link down netlink event message (nlmsg) was dropped or lost. Due to this lack, DCBX could not negotiate and Fibre Channel over Ethernet (FCoE) did not login to the fabric in this case. This update resolves this

problem. Now, lldpad successfully initiates a Data Center Bridging Exchange (DCBX).

BZ#647833

Previously, lldpad could not be upgraded or removed on systems which had lldpad packages for both Intel P6 and Intel 64 simultaneously installed. As a workaround, this update removes such packages with the command rpm -e --noscripts.

BZ#694671

Previously, non-default priorities for FCoE did not correctly work, because lldpad handled application type-length-values (TLV) incorrectly. With this update, non-default priorities work as expected.

BZ#694925

Previously, lldpad did under certain circumstances not correctly synchronize with peers on link events. Due to this issue, users had to manually reset the link or lldpad. This update resolves the synchronization issue. Now, synchronization with peers on link events works as expected.

Enhancement

BZ#675076

The lldpad package has been upgraded to upstream version 0.9.41, which builds on the new kernel interface and adds support for 802.1Qbg Edge Virtual Bridging, netlink, and libvirt, as well as a new, flexible build process.

All lldpad users are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

1.149.2. RHBA-2012:0027 — lldpad bug fix and enhancement update

An updated lldpad package that fixes multiple bugs and adds multiple enhancements is now available for Red Hat Enterprise Linux 6 Extended Update Support.

The lldpad package provides the Linux user space daemon and configuration tool for Intel's Link Layer Discovery Protocol (LLDP) agent with Enhanced Ethernet support.

The lldpad package has been upgraded to upstream version 0.9.43, which includes all of the bug fixes and enhancements addressed in the RHBA-2011:1604 lldpad bug fix and enhancement advisory for Red Hat Enterprise Linux 6.1. For the sake of convenience, those fixes and enhancements are detailed below. (BZ#769783)

Bug Fixes

BZ#749057

The Brocade 8000 Fibre Channel Forwarder (FCF) switch with FabOs 6.4.2b failed to process the CEE TLV frame on fabric session startup (started by the llpad). As a consequence, the Brocade 8000 Fibre Channel Forwarder (FCF) switch with FabOs 6.4.2b terminated the connection and subsequent fabric logins failed when IEEE 802.1Qaz DCBX was enabled. With this update, the llptool utility can configure lldpad not to use the CEE TLV frame for the fabric session initiation (for the eth3 device, the initiator should issue the "lldptool -T -i eth3 -V IEEE-DCBX mode=reset" command) and the problem no longer occurs.

BZ#694639

The lldpad service triggered excessive timeout events every second. This caused the service to

consume excess resources. Now, the lldpad service has been switched from polling-based to a demand-based model. This prevents excessive timeout event generation and ensures that the service consumes only the expected resources.

BZ#733123

The lldpad utility did not detect the maximum number of traffic classes supported by a device correctly. This resulted in an invalid or incorrect hardware configuration. Now, the utility detects the maximum number of traffic classes correctly.

BZ#720825, BZ#744133

The Edge Control Protocol (ECP) could not verify whether a port lookup was successful when running Virtual Discovery and Configuration Protocol (VDP) on bonded devices because VDP does not support bonded devices. As a consequence, the LLDP agent terminated unexpectedly with a segmentation fault. With this update, VDP is no longer initialized on bonded devices and the crash no longer occurs.

BZ#647211

The lldpad utility failed to initialize correctly on the Intel 82599ES 10 Gigabit Ethernet Controller (Niantic) with virtual functions enabled and returned a message that there were too many neighbors. With this update, lldpad initializes correctly and the problem no longer occurs.

BZ#735313

Prior to this update, a user with non-superuser permissions could start the lldpad service. With this update the lldpad init scripts have been modified and a user with non-superuser permissions can no longer start the service.

BZ#683837

The init script did not perform a line feed when returning the output of a service command. With this update, the init script has been recoded and the output of the service command is correct.

BZ#720730

The get_bcn() function returned without freeing the nlh variable, which caused a memory leak. The function has been modified and the memory leak no longer occurs.

BZ#741359

The lldpad daemon failed to detect that a NIC (Network Interface Card) had the offloaded DCBX (Data Center Bridging eXchange) stack implemented in its firmware. As a consequence, the lldp packets were sent by both, the daemon and the NIC. With this update, the lldpad daemon no longer sends the packets if a NIC driver implements the offloaded DCBX stack.

BZ#749943

The lldpad utility incorrectly accessed memory. With this update, the utility accesses the memory correctly.

Enhancement

BZ#695550

The lldpad package now supports the 802.1Qaz standard (Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes).

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

1.149.3. RHBA-2011:1381 — lldpad bug fix update

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

The lldpad package provides the Linux user space daemon and configuration tool for Intel's Link Layer Discovery Protocol (LLDP) Agent with Enhanced Ethernet support.

Bug Fix

BZ#739851

Previously, the Edge Control Protocol (ECP) could not verify whether a port lookup was successful when running Virtual Discovery and Configuration Protocol (VDP) on bonded devices because VDP does not support bonded devices. As a consequence, the LLDP agent terminated unexpectedly with a segmentation fault. With this update, VDP is no longer initialized on bonded devices and the crash no longer occurs.

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

1.149.4. RHBA-2011:0821 — lldpad bug fix update

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

The lldpad package contains the Linux user space daemon and configuration tool for Intel Link Layer Discovery Protocol (LLDP) Agent with Enhanced Ethernet support for the Data Center.

Bug Fix

BZ#701993

Previously, the lldpad service triggered excessive timeout events every second. This caused the service to consume excess resources. With this update, the lldpad service has switched from polling-based to a demand-based model. This prevents excessive timeout event generation and ensures the service consumes only the expected resources.

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

1.150. lohit-devanagari-fonts

1.150.1. RHEA-2011:0203 — lohit-devanagari-fonts enhancement update

An updated lohit-devanagari-fonts package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The lohit-devanagari-fonts package provides a free Devanagari Script TrueType and OpenType font.

Enhancement

BZ#651713

A glyph for the Indian rupee sign (U+20B9) defined in version 6.0 of the Unicode standard has been added to the font.

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

1.151. lohit-kannada-fonts

1.151.1. RHBA-2011:0667 — lohit-kannada-fonts bug fix and enhancement update

An updated lohit-kannada-fonts package that corrects display problems and adds Latin punctuation glyphs is now available.

lohit-kannada-fonts provides a free TrueType and OpenType typeface for writing and displaying Kannada script.

Bug Fix

BZ#577127

Previously, Lohit Kannada did not include Latin punctuation glyphs (such as opening and closing parentheses). When these characters were required while using the Kannada script, they were drawn from a system's default Latin script. With this update, these characters have been added to the Kannada character set, improving the look of text which mixes Kannada characters and Latin punctuation glyphs.

As well, the right-side bearing rules for Kannada conjuncts that immediately follow a Latin parenthesis character have been corrected to ensure these glyphs no longer kern so close as to overlap.

All users of lohit-kannada are advised to upgrade to this updated package, which fixes this bug.

1.152. lohit-oriya-fonts

1.152.1. RHBA-2011:0707 — lohit-oriya-fonts bug fix update

An updated lohit-oriya-fonts package that fixes OpenType rules for presenting conjunction characters in Qt-based applications is now available for Red Hat Enterprise Linux 6.

The lohit-oriya-fonts package provides a free Oriya script TrueType and OpenType font.

Bug Fix

BZ#623990

Oriya script is an abugida or alphasyllabic writing system and, when certain consonant glyphs would otherwise be written adjacent, applies rules for replacing the glyphs with a single, ligatured conjunction character. The OpenType version of Lohit Oriya did not, previously, apply these rules correctly when the typeface was used in an application built using the Qt application framework (eg OpenOffice or KWrite). With this update, these rules act as expected, and conjunct symbols appear properly when the OpenType face is used in Qt-based applications.

Note: this bug did not present if the TrueType face was used in Qt-based applications, nor did it present in applications built with the GTK+ framework (eg AbiWord and gedit) if the OpenType face was used.

Users should upgrade to this updated package, which resolves this issue.

1.153. lohit-tamil-fonts

1.153.1. RHBA-2011:0704 — lohit-tamil-fonts bug fix update

An updated lohit-tamil-fonts package that fixes a display issue in the asterisk glyph ('*' -- Unicode U+002A) is now available for Red Hat Enterprise Linux 6.

The lohit-tamil-fonts package provides a free Tamil script TrueType and OpenType font.

Bug Fix

BZ#629813

The Latin asterisk glyph ('*' -- ASCII 0x2A; Unicode U+002A) was over-sized relative to the same glyph as presented in other non-Latin scripts which include Latin glyphs (eg Lohit Devanagari). With this update, the asterisk has been re-drawn to match the glyph included with Lohit Devanagari. This re-drawing also ensures the asterisk matches the typographic 'color' of the Tamil script characters and the other Latin glyphs included with this typeface.

Users should upgrade to this updated package, which resolves this issue.

1.154. lsvpd

1.154.1. RHEA-2011:0547 — lsvpd enhancement update

An updated lsvpd package that adds an enhancement is now available available for Red Hat Enterprise Linux 6.

The lsvpd package contains all of the lsvpd, lscfg and lsmcode commands.

Enhancement

BZ#632737

This update upgrades the lsvpd package to upstream version 1.6.9, which provides an enhancement over the previous version.

Users of lsvpd are advised to upgrade to this updated package, which adds this enhancement.

1.155. luci

1.155.1. RHBA-2011:0655 — luci bug fix and enhancement update

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

The luci package provides a web-based high-availability cluster configuration application.

Bug Fixes

BZ#536841

Previous versions of **luci** did not allow users to change the number of votes for a particular node. With this update, the underlying source code has been adapted to provide this functionality, and users are now allowed to change the number of votes for a node as expected.

BZ#600057

Under certain circumstances, the list of nodes may not have included uptime information for all nodes. This error has been fixed, and the uptime is now displayed for all listed nodes as expected.

BZ#600078

Prior to this update, the user interface of the **luci** application did not inform users about possible issues with using the Quorum Disk on certain configurations. This update corrects this error, and the user interface now informs users that Quorum Disk cannot be used unless each node has exactly 1 vote, and advises them not to use this feature for clusters with more than 8 nodes.

BZ#605932

When configuring the Quorum Disk, previous version of **luci** did not allow users to reset input fields to their default values. To address this issue, this update adds the **`Reset values to defaults`** button to the user interface.

BZ#613155

Previously, when a user other than **`root`** or **`luci`** attempted to run the **luci** init script, the service failed to start and a traceback was written to standard error. With this update, the init script has been corrected to terminate with exit code 4 in this case.

BZ#613871

When a user attempted to view a cluster that contained an unknown or unsupported fence device, **luci** displayed error 500, and a traceback was written to the **`luci.log`** log file. This error has been fixed, and **luci** now correctly displays “Unknown fence device type” when an unknown or unsupported fence device is encountered.

BZ#614963

Due to an incorrect use of a deprecated Python feature, the following message may have been occasionally written to the **`luci.log`** log file:

```
DeprecationWarning: BaseException.message has been deprecated as of
Python 2.6
```

This update corrects the underlying source code not to use deprecated features, so that the above message no longer appears in the log file.

BZ#616239

Previously, deleting a cluster from the user interface only removed the cluster from **luci**, but did not remove the **`cluster.conf`** configuration file or shut down the clustering on the nodes. This update corrects this error, and users are now allowed to completely destroy a whole cluster by selecting all of its nodes and clicking the **`Delete`** button.

BZ#617586

Prior to this update, certain actions, such as the creation of a new cluster, required users to manually refresh the user interface. This update introduces a progress dialog that informs users about the current status of long-running operations and automatically refreshes the user interface when such an

operation completes.

BZ#617587

When the **ricci** daemon encountered an error, previous version of **luci** did not present this error to a user and displayed a generic error message instead. In order to make it easier to determine the cause of such errors, this update adapts **luci** to display the error messages reported by **ricci**.

BZ#618701

When a user created a cluster with a name that contained spaces, clicking the cluster name in the user interface caused **luci** to display error 404. This error has been fixed, and **luci** is now able to work with clusters with spaces in their names as expected.

BZ#620377

Prior to this update, various drop-down menus in the user interface of **luci** did not remember their selection. With this update, this error no longer occurs, and all drop-down menus now remember their selection as expected.

BZ#622562

Previous versions of **luci** did not allow users to configure unfencing, and thus prevented the SAN fencing agents and **fence_scsi** from being unfenced at boot time. With this update, the underlying source code has been adapted to provide this functionality, and users are now allowed to configure unfencing from the user interface.

BZ#624716

When a user configured a cluster for the first time, the **Services**, **Resources**, **Failover Domains**, and **Devices** tabs contained the following error message:

```
No nodes from this cluster could be contacted. The status of this
cluster is unknown.
```

Since this message may have been misleading, **luci** has been adapted to display a more comprehensive message, such as “No items to display”.

BZ#633983

Prior to this update, **luci** did not handle the **nodename** parameter for the **fence_scsi** fence agent correctly. This update corrects this error, and the **nodename** parameter is now handled properly.

BZ#636267

Prior to this update, the **Fence Devices** tab contained two **Update** buttons. However, these buttons are no longer required, and clicking them did not trigger any action. With this update, the **Update** buttons have been removed from the **Fence Devices** tab.

BZ#636300

Previously, **luci** did not handle the username for the **fence_egenera** fence agent correctly. With this update, the underlying source code has been modified to address this issue, and the username for **fence_egenera** is now handled correctly.

BZ#639123

Prior to this update, action buttons such as those for starting, stopping, deleting, or rebooting nodes

were active even if no node was selected. Consequent to this, clicking such a button caused **luci** to display an error message. This update addresses this issue, and the action buttons are no longer active when no node is selected.

BZ#639124

When changes to a cluster were made outside of **luci**, previous versions of **luci** did not update the local database to reflect the current cluster membership. This update corrects this error, and in response to such changes to cluster membership, **luci** now updates its local database as expected.

BZ#659014

Previously, when a user attempted to configure a node with a *fully qualified domain name* (FQDN) that did not match the cluster node name, **luci** incorrectly displayed error 500, and a traceback was written to the **`luci.log`** log file. This error no longer occurs, and users are now allowed to configure such nodes as expected.

BZ#678366

Under certain circumstances, an attempt to remove existing fence methods from a device, or add new fence instances may have failed. This update corrects the fence management in **luci**, and removing existing fence methods from a device or adding new fence instances no longer fails.

BZ#678424

Under certain circumstances, an attempt to add a node to an existing cluster could fail with the following message written to the **`luci.log`** log file:

```
AttributeError: 'ClusterNode' object has no attribute 'getID'
```

With this update, the underlying source code has been modified to address this issue, and **luci** no longer fails with the above error when adding a new node to a cluster.

BZ#682843

Previously, when configuring the **Samba** resource agent, the user interface of **luci** contained the **`Workgroup`** input box. Since, this option is not used by the resource agent, this update removes it from the user interface.

Enhancements

BZ#472972

Support for the **`OracleListener`** and **`OracleInstance`** resource agents has been added.

BZ#557234

This update allows **luci** to communicate with the **`ricci`** daemon on an interface different from the one that is used for the cluster communication.

BZ#620343

To make the distinction between “services” and “resources” more obvious, the **`Services`** label in the user interface of **luci** has been replaced with more comprehensive **`Service Groups`**.

BZ#620373

The user interface of **luci** has been adjusted to present tabs to a user in more logical order.

BZ#624558

The **Use UDP unicast (UDPU)** option has been added to the **Network Configuration** page. Note that unless expert mode is enabled, the **Use broadcast** option is no longer presented to a user.

BZ#632344

This update introduces the **Logging Configuration** page, which allows users to configure centralized logging.

BZ#637223

Support for the **fence_cisco_ucs** fence agent has been added.

BZ#639107

Support for the **fence_rhev** fence agent has been added.

BZ#639111

This update adds support for configuring non-critical cluster resources.

BZ#639120

An expert user mode has been added. When enabled, this mode allows users to edit most of the properties that are defined by the cluster schema.

BZ#666971

This update adds the **Disable updates to static routes** check box to the user interface, allowing users to disable updates to static routes in the IP resource agent.

BZ#680173

Support for the *Distributed Replicated Block Device* (DRBD) resource type has been added.

BZ#681506

This update re-includes **fence_brocade** to the list of supported fence agents.

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

1.156. lvm2

1.156.1. RHBA-2011:0772 — lvm2 bug fix and enhancement update

Updated lvm2 packages that fix several bugs and add enhancements are now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

Bug Fixes

BZ#683689

Fixes a possible endless loop in cache.

BZ#677739

Fixes a deadlock while removing last exclusive snapshot in cluster.

BZ#675744

Fixes a boot failure on big-endian architectures.

BZ#674823, BZ#687857

Adds device-mapper library support for wiping ioctl buffers in kernel.

BZ#672617

Improves insufficient free space message for lvcreate.

BZ#660471

Fixes the use of --addtag --deltag arguments for pvchange in cluster.

BZ#660467

Adds support for multiple --addtag or multiple --deltag arguments for pvchange.

BZ#654441

Adds lvm2app support for querying float attributes.

BZ#649334

Fixes lvcreate to not exit incorrectly with a failure if --test option is used.

BZ#648219

Fixes vgs to not limit the number of tags displayed.

BZ#647167

Adds a possibility to use --addtag and --deltag arguments in one command.

BZ#645488

Fixes I/O errors for merged snapshots on boot.

BZ#642575

Fixes a possible error in processing a regular expression used in device filter.

BZ#642938

Adds a new global/metadata_read_only configuration option to disallow any operations changing metadata.

BZ#638052, BZ#652200

Fixes incorrect detection of mounted filesystem in fsadm script.

BZ#636006

Adds scalability improvements.

BZ#635949

Clarifies the description in lvconvert man page.

BZ#634349

Adds support for /, =, !, :, #, & in tags.

BZ#633033

Fixes an issue where adding VG tags left metadata corrupted.

BZ#633018

Adds support for multiple --addtag and --deltag arguments within a single command.

BZ#633013

Adds support for up to 1024 characters in LV tags.

BZ#632681

Fixes cmirrord init script to not fail if it is already started.

BZ#625192

Fixes a failure in mirror log allocation if a device failure in the log is encountered.

BZ#625135

Fixes an issue that caused a mirror log to be removed while replacing the failed mirror image.

BZ#623218

Fixes pvremove to not show 'No physical volume label read' message when removing PVs with no metadata copies in one pvremove command.

BZ#621281

Fixes lvconvert to honour the --yes and --force options.

BZ#620571

Fixes a regression where a non-root user could not view LVM2 devices.

BZ#615907

Fixes a failure in rename during metadata archive and backup handling.

BZ#614049

Includes hooks for querying and setting pvs, vgs and lvs report fields in lvm2app.

BZ#613829

Fixes an issue where a mirror containing snapshot volumes could end up with I/O hung if there was a failed device.

BZ#612862

Fixes clvmd to clean up dlm lockspace if clvmd restart is invoked.

BZ#607334

Adds a possibility to use the allocate fault policy for mirrored logs.

BZ#603912, BZ#602748

Disallows adding a mirror log and removing mirror images (or vice versa) in one step while specifying PVs.

BZ#602389

Clarifies a message about pvmove operation if another process finishes or aborts it.

BZ#601740

Improves lvscan man page to describe possible output values.

BZ#601383

Disallows converting a mirrored log to core log along with image conversion while specifying PVs.

BZ#595507

Fixes an issue with clustered mirrors and very slow I/O.

BZ#596352

Adds new -f option to clvmd to run it in foreground.

BZ#553381

Fixes clvmd init script to comply with LSB and Red Hat init script guidelines.

BZ#525972

Reduces delays by avoiding scans on failed devices (devices/disable_after_error_count configuration option).

BZ#525957

Adds support for snapshots of a mirror.

BZ#510292

Adds support for striped mirrors.

BZ#504871

Adds 'cling by tags' allocation policy.

Users are advised to upgrade to these updated lvm2 packages, which resolve these issues and add these enhancements.

1.157. m17n-contrib

1.157.1. RHEA-2011:0915 — m17n-contrib enhancement update

Updated m17n-contrib packages that add an enhancement are now available for Red Hat Enterprise Linux 6.

The m17n-contrib package contains contributed multilingualization (m17n) data files for the m17n-lib project.

Enhancement

BZ#712120

On Indian keyboard layouts, users were unable to enter the newly added Rupee Unicode symbol (U+20B9). With this update, the symbol has been added as a "Alt_Gr+4" keyboard shortcut in the InScript (Indian Script) keymap, where Alt_Gr is the right Alt key.

Users of m17n-contrib are advised to upgrade to these updated packages, which add this enhancement.

1.157.2. RHBA-2011:0544 — m17n-contrib bug fix and enhancement update

An updated m17n-contrib package that includes two corrected keymap files and two improved keymap files, each back ported from upstream, is now available.

This package contains contributed internationalization files for m17n-lib.

Bug Fixes

BZ#653782

Previously, when using the Devanagari script keymap -- hi-remington.mim -- the key combination to produce "■■" (the respectful form of the second person pronoun) on qwerty keyboards was "Shift-h backspace w [backspace". The widely used sequence for this pronoun, however, is "Shift-h k w [k" (with "k" used rather than the backspace). With this update the more common key sequence is now used by the hi-remington.mim keymap file.

BZ#653783

The Malayalam script keymap -- ml-inscript.mim -- was missing the 20th letter, ■ (ca). This is mapped to the semi-colon (;) on qwerty keyboards. Previously, when the Malayalam input system was active, pressing that key (either physically or using the on-screen keyboard) produced no output. The on-screen keyboard also displayed a blank keycap. This update corrects the typo in the ml-inscript.mim keymap file. When the Malayalam input method is used "ca" displays on the on-screen keyboard and appears in documents when typed, as expected.

Enhancements

BZ#642138

The Telugu script keymap -- te-inscript.mim -- now maps three further Telugu script characters to English-language keyboard keys. The specific changes are as follows: the vowel character U0c60 ("■") is now mapped to the pipe symbol ("|"); the dependent vowel character U0c44 ('■■') is now mapped to the back slash ("\"); and the dependent vowel character U0c01 ("■■") is now mapped to the capital X ("X").

BZ#653781

The Tamil script keymap -- ta-tamil99.mim -- now maps seventeen further input options for generating both Tamil and English script glyphs on English-language keyboards. With the updated keymap file installed and active, the "f" key now generates a question mark ("?"). The other sixteen added options are Control+[key] inputs. They include new input options to generate several English

characters such as the copyright symbol (using Control+c), the bullet character (Control+.) and single and double typographer's quote marks (using Control+7 through Control+9). As well, eight further Tamil script glyphs can now be generated, using Control+q +s +w +d +e +g +t and +r.

All users, especially those inputting Devanagari, Malayalam, Telugu or Tamil script characters, should install this update, which addresses these issues and adds these enhancements.

1.158. m17n-lib

1.158.1. RHEA-2011:0916 — m17n-lib enhancement update

An updated m17n-lib package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The m17n-lib package contains a multilingual text library used primarily to allow the input of many languages with the input table maps from the m17n-db and m17n-contrib packages.

Enhancement

BZ#712118

On Indian keyboard layouts, users were unable to enter the newly added Rupee Unicode symbol (U+20B9). With this update, the Alt_Gr (right Alt) key is supported, and it is now possible to map the Rupee symbol on a keyboard shortcut such as "Alt_Gr+4".

Users of m17n-lib are advised to upgrade to this updated package, which adds this enhancement.

1.159. man-pages

1.159.1. RHBA-2011:0679 — man-pages bug fix and enhancement update

An updated man-pages package that corrects several documentation errors and omissions and adds several improved man pages is now available for Red Hat Enterprise Linux 6.

The man-pages package provides man (manual) pages from the Linux Documentation Project (LDP).

Bug Fixes

BZ#634626

The sd man page had an invalid link referring to the scsi man page. With this update, all references to the scsi man page were removed from the sd man page.

BZ#669768

The "getent --help" command output mentioned a "-s" switch which was not explained anywhere in the getent man page. Since the getent man page is outdated, the entire page was removed for this update.

BZ#678376

The man page for clock_gettime had references to the CLOCK_REALTIME_HR and CLOCK_MONOTONIC_HR constants, that were used in clock_getres.2, clock_gettime.2, clock_nanosleep.2, clock_settime.2, and timer_create.2. These constants are no longer present in the Linux kernel and clock_gettime was corrected to remove all references to these constants.

BZ#679530

A typographical error in the SHA, MD5, and DES algorithms on crypt(3) man page, meant key significance in passwords was presented incorrectly. The typo was fixed for this update.

BZ#679894

Information about a new keyword -- scopev4 -- was missing from the "gai.conf" man page. As of this update, "gai.conf(5)" now documents the scopev4 keyword.

BZ#683039

The example code demonstrating how to use the getifaddrs() API in the getifaddrs man page contained a bug capable of crashing getifaddrs if used. The previous example code did not check for a NULL pointer under certain conditions which would cause a segmentation fault. With this update the example code tests for this condition, as expected, thereby avoiding the segfault.

Enhancements

BZ#528546

The man pages for "pwrite(v)" and "pread(v)" were previously not included in the man page package. With this update, they are.

BZ#613777

The "get_mempolicy" man page was updated to be more contemporaneous with the version of the Linux kernel (version 2.6.32) used by Red Hat Enterprise Linux 6.

BZ#634986

The "pthread_attr_setguardsize" man page was updated to include information about glibc 2.8 changes.

All users of manual pages are advised to upgrade to this updated package, which resolves these issues.

1.160. man-pages-ja

1.160.1. RHBA-2011:0192 — man-pages-ja bug fix update

An updated man-pages-ja package that fixes three bugs is now available for Red Hat Enterprise Linux 6.

The man-pages-ja package contains Japanese translations of the Linux Documentation Project man pages.

Bug Fixes

BZ#579647

Previously, the man-pages-ja package contained the outdated Japanese manual pages based on SysVinit which is not shipped in Red Hat Enterprise Linux 6. This update drops those redundant manual pages to avoid a confusion.

BZ#600324

Previously, the Japanese manual page of the 'snmpd.conf' did not mention the deprecated notice for the listening port specifier in the sink directives.This update adds the deprecated notice.

BZ#618934

Previously, the Japanese manual page of the 'echo' command did not mention the format of '\e' and '\xHH' in the -e option. The updated package adds the description of '\e' and '\xHH'.

BZ#628891

Previously, the Japanese manual page of the 'pmap' command did not mention the "extended and device format fields". This update adds the description of it.

All man-pages-ja users are advised to upgrade to this updated package, which resolves these issues.

1.161. man-pages-overrides

1.161.1. RHBA-2011:0780 — man-pages-overrides bug fix and enhancement update

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

A collection of manual ("man") pages to complement other packages or update those contained therein.

This updated man-pages-overrides package provides fixes for the following bugs:

Bug Fixes

BZ#540492, BZ#636785

The semanage(8) manual page has been rewritten.

BZ#604626

Several typographical errors have been fixed in the yum-verify(1) manual page.

BZ#615873

The release tag has been fixed in the w3m(1) manual page.

BZ#619779

The missing description for the auto-rename option has been added to the lftp(1) manual page.

BZ#622451, BZ#638625, BZ#644308, BZ#673968

The logrotate(8) manual page has been updated, fixing multiple issues such as missing options, typographical errors, an incorrect author tag, and a faulty description of the "size" parameter.

BZ#632081

The Japanese version of the man(1) manual page no longer contains a duplicate line in the specification of the "-p pager" option

BZ#633701

Several syntax errors and typographical errors have been fixed in the expect(1) manual page.

BZ#650162

The information on home directories in the useradd(8) manual page has been fixed.

BZ#651120

The "-v" option in the parametersetfattr(1) manual page is now described more extensively to prevent possible confusion.

BZ#657563

The find(1) manual page has been rewritten.

BZ#658734

The setfacl(1) manual page has been update to address various issues.

BZ#675213

A typographical error has been fixed in the userpasswd(1) manual page.

BZ#675223

Several typographical errors have been fixed in the locate(1) manual page

BZ#675682

Several typographical errors have been fixed in the pcregrep(1) manual page.

BZ#675688

Several typographical errors have been fixed in the pcretest(1) manual page.

BZ#676540

Several typographical errors have been fixed in the magic(5) manual page.

Enhancements

BZ#613979

The dftest(1) and randpkt(1) manual pages are now available.

BZ#615905

The ospfclient(8) and watchquagga(8) manual pages are now available.

Users are advised to upgrade to this updated man-pages-overrides package, which resolves these issues and adds these enhancements.

1.162. mcelog

1.162.1. RHBA-2011:0519 — mcelog bug fix update

An updated mcelog package that fixes various bugs is now available.

mcelog is a daemon that collects and decodes Machine Check Exception data on AMD64 and Intel 64 machines.

Bug Fixes

BZ#614874

The mcelog service did not check whether another instance of mcelog was running, which could result in multiple mcelog service instances on a single system. This could result in lost or over-reported Machine Check Exceptions. mcelog now detects whether another instance is already running, preventing multiple instances from being launched on a single system simultaneously.

BZ#646568

When a Machine Check Error occurs, a message indicating that the issue is not a software problem is output to the console. This incorrectly implies that a hardware problem exists. The message has now been corrected to indicate that a Hardware Event has occurred, instead.

BZ#647066

No configuration file was provided for mcelog, preventing users from configuring mcelog daemon and its actions. A default configuration file (/etc/mcelog/mcelog.conf), which can be used to modify the behavior of mcelog at runtime, is now provided.

BZ#664016

Support for future Intel processors has been added to mcelog, enabling mcelog to decode Machine Check Exceptions for these processors when they become available.

BZ#682753

The default mcelog configuration file contained references to files that did not exist in the default package installation. This caused mcelog to attempt to execute files that did not exist. The mcelog configuration file has been corrected. Note that this bug was reported and corrected during development, and was not seen in production systems in the field.

All users of mcelog are advised to upgrade to this updated mcelog package, which resolves these issues.

1.163. mdadm

1.163.1. RHBA-2011:0759 — mdadm bug fix and enhancement update

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

mdadm is a utility for creating, managing, and monitoring Linux MD (multiple disk) devices.

Bug Fixes

BZ#605710

Previously, the "noiswmd" kernel command line option did not set the rd_NO_MDIMSM variable to 1 and the udev rules thus failed to match the option. This update removes the rule for the rd_NO_MDIMSM variable and adds the "noiswmd" and "nodmraid" command line options, which substitute the rule for rd_NO_MDIMSM.

BZ#626762

The md kernel module stopped responding when attempting to stop a RAID device. This occurred due to a mutex deadlock. With this update, the underlying code was changed and the issue no longer occurs.

BZ#636883

Previously, mdadm did not accept the short version of the "--export" (that is "-Y") and "--name" (that is "-N") options. This was due to missing entries in the list of short options. With this update, the missing entries have been added and the short versions of the options now work as expected.

Enhancements

BZ#633306

Previously, mdadm was not able to rebuild newly-connected drives automatically. This update adds the array auto-rebuild feature and allows a RAID stack to automatically rebuild newly-connected drives.

BZ#633667

RAID migration is now supported: mdadm is now able to change the RAID level of an already-existing device.

BZ#633671

Previously, mdadm could not add a new disk to an already-existing volume. This update adds the OLCE (On Line Capacity Expansion) feature, which allows mdadm to add new disks to an array and allocate their resources to existing volumes.

BZ#633688

Previously, mdadm did not track the progress of the rebuild and level-migration operations and therefore was not able to recover their progress after a system failure. This update adds the check-pointing feature, which tracks their progress and allows mdadm to resume these operations after a system failure from the last check point.

BZ#633690

This update adds SAS-SATA feature, which allows the user to disconnect a set of SATA (Serial Advanced Technology Attachment) drives from a SCSI Controller Unit (SCU) and connect it to an Advanced Host Controller Interface (AHCI) and vice versa.

BZ#633692

This update limits the RAID-5 support for volumes on drives attached to the SCU on systems with the X79 chipset (code-named "Patsburg"). It inhibits the creation, assembly, activation, and level migration of RAID 5 volumes on drives attached to the SCU on these systems.

Users are advised to upgrade to this updated mdadm package, which resolves these issues and adds these enhancements.

1.163.2. RHBA-2011:1126 — mdadm bug fix update

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

The mdadm package contains a utility for creating, managing, and monitoring Linux MD (multiple disk) devices.

Bug Fixes

BZ#723135

When an array was changing level from redundant to non-redundant such as RAID 0, mdadm failed to exit and remained in memory. This caused a variety of issues, including a termination with a

segmentation fault when two array transitions were executed sequentially. With this update, a patch has been provided to address this issue, and the monitor is now properly removed from memory after the backward takeover operation.

BZ#723137

If an array size was not properly aligned to the chunk size, the expansion process failed to start and the "New chunk size does not divide component size" error message was returned. This bug has been fixed, and the array alignment is now checked before the expansion process begins.

BZ#723139

Previously, when a volume was created with the "--size" option but without providing a chunk size and a container, mdadm used the "UnSet=65534" option for rounding the volume size before setting the default chunk size. This caused the new volume to be created with an incorrect size. This bug has been fixed, and the volume size is now properly rounded to the chunk size.

BZ#723140

When the expansion process of a RAID 0 volume was restarted, mdadm failed to correctly assemble the array because the critical section could not be restored from a backup file, and the "mdadm: Failed to restore critical section for reshape - sorry" error message was returned. A patch has been provided to address this issue, and now, the RAID 0 expansion process cannot be restarted, thus fixing this bug.

BZ#723141

Previously, mdadm incorrectly calculated reshape start data disks number (0) during the reshape restart operation and used it for calculations. This caused a variety of issues; for example, when two disks were added to the 3-disk RAID 5 array and the array under migration was disassembled and then assembled again, mdadm terminated unexpectedly. A set of patches has been provided to address this issue, and the reshape process is now properly restarted in the described scenario.

BZ#723142

When two arrays were configured in a container and the arrays were reassembled during a rebuild or initialization process, the stored checkpoint for one of the arrays was sometimes lost. Consequently, the restarted process did not use the checkpoint information and started from zero position instead. A patch has been provided to address this issue, and the restarted process now properly continues from the stored checkpoint.

Users of mdadm are advised to upgrade to this updated package, which fixes these bugs.

1.164. memtest86+

1.164.1. RHBA-2011:0683 — memtest86+ bug fix and enhancement update

An updated memtest86+ package that fixes one bug and adds an enhancement is now available for Red Hat Enterprise Linux 6.

The memtest86+ package contains an advanced memory diagnostic tool for x86, AMD64 and Intel 64 computers. BIOS-based memory tests are only a quick check and often miss many of the failures that are detected by memtest86+.

Bug Fix

BZ#607006

The memtest86+ tool failed to start on AMD64 and Intel 64 computers with the "--type=netbsd /elf-memtest86+-4.00" kernel parameter, and the "Error 13: Invalid or unsupported executable format" error message was given. This option now works as expected, and no error message is displayed.

Enhancement

BZ#640731

With this update, memtest86+ supports the latest Intel processors, including those based on the Intel Xeon Processor E56XX, L56XX, W36XX and X56XX families, and the Intel Xeon Processor E7 family.

Users of memtest86+ are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

1.165. mesa

1.165.1. RHEA-2011:0628 — mesa enhancement update

Updated mesa packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

Mesa provides a 3D graphics application programming interface (API) that is compatible with OpenGL (Open Graphics Library). It also provides hardware-accelerated drivers for many popular graphics chips.

Enhancement

BZ#667563

This update adds accelerated 3D support for systems based on the 2nd Generation Intel Core Processor Family to the mesa packages and provides updated drivers for all other supported 3D hardware.

All Mesa users are advised to update to these upgraded packages, which add this enhancement.

1.166. microcode_ctl

1.166.1. RHEA-2011:0712 — microcode_ctl enhancement update

An updated microcode_ctl package that provides several enhancements is now available for Red Hat Enterprise Linux 6.

The microcode_ctl package provides microcode updates for Intel processors.

Enhancements

BZ#638286

The Intel CPU microcode file is updated to version 20101123. This is the most recent version of the microcode available from Intel.

BZ#578107

microcode_ctl is now udev-driven and the previously delivered init.d script is no longer needed.

Note that the system must be rebooted in order for these changes to take effect.

All users of Intel processors are advised to upgrade to this updated package, which adds these enhancements.

1.167. mipv6-daemon

1.167.1. RHBA-2011:0741 — mipv6-daemon bug fix and enhancement update

An updated mipv6-daemon package that fixes several bugs and adds various enhancements is now available.

The mipv6-daemon package contains a mobile IPv6 service for clients, which allows them to relocate within an IPv6-enabled network yet remain reachable

The mipv6-daemon package has been upgraded to upstream version 2.0.2.20110203b, which provides numerous bug fixes and enhancements over the previous version. (BZ#612007)

Users are advised to upgrade to this updated mipv6-daemon package, which resolves these issues and adds these enhancements.

1.168. mksh

1.168.1. RHBA-2011:0580 — mksh bug fix and enhancement update

An updated mksh package that fixes three bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The mksh package provides the MirBSD version of the Korn Shell which implements the ksh-88 programming language for both interactive and shell script use.

Bug Fixes

BZ#616771

Previously, mksh did not handle trace output correctly. Due to this problem, mksh aborted unexpectedly when the tracing was enabled and a long string was to be reported, This update improves the long trace output handling. Now, long trace output is successfully printed without interruption.

BZ#616777

Previously, mksh did not handle aliases that contained aliases correctly. Due to this problem, mksh aborted when double aliases were used. This update corrects the alias handling code. Double aliases are handled as expected.

BZ#618274

Previously, bad substitution could abort mksh unexpectedly because of a conflict between acceptable code for ksh-88 and ksh-93. This update recognizes both code types and prints errors as expected.

Enhancement

BZ#659668

Previously, users had to change the shebang in their ksh-88 scripts or port their scripts to ksh-93. This update adds the "alternatives" switching method that allows to switch between ksh-93 provided by the ksh package and ksh-88 provided by the mksh package for /bin/ksh. Now, users can apply

their scripts without modification or porting them to ksh-93 one by one.

All users of mksh are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

1.168.2. RHBA-2011:0645 — ksh bug fix and enhancement update

An updated ksh package that fixes several bugs and adds various enhancements is now available.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories -- a shell programming language upwards-compatible with "sh" (the Bourne Shell).

This updated ksh package provides fixes for the following bugs:

Bug Fixes

BZ#616684

When a ksh script contained the "trap" command to capture a "SIGPIPE" signal, sending this signal via the built-in "echo" command could cause its output to be incorrectly added to the redirected output of an external command. With this update, ksh now flushes the output buffer before redirecting any output streams.

BZ#616691

Due to incorrect signal handling, receiving a signal while still processing the same one caused ksh to terminate unexpectedly with a segmentation fault. With this update, the subsequent signals are deferred until the current one is processed; thus, ksh no longer crashes.

BZ#619692

The previous version of the ksh man page contained an unavailable "-m" option and an insufficient description of the "-R" option. In this updated version of the man page, the section mentioning the unavailable option is removed and the description of the "-R" option is extended.

BZ#637052

Assigning a value to an array variable during the execution of the "typeset" command could cause ksh to terminate unexpectedly with a segmentation fault. This update corrects the array handling in this command and ksh no longer crashes.

BZ#643811

Prior to this update, ksh did not close a file containing an auto-loaded function definition. After loading several functions, ksh could have easily exceeded the system's limit on the number of open files. With this update, files containing auto-loaded functions are properly closed, thus, the number of opened files no longer increases with usage.

BZ#644362

If a here document (heredoc — specifies a string literal in command line shells) was combined with an auto-loaded function, interference with the here document processing could occur causing output to be truncated to 8 kB. This update improves the here document processing logic and auto-loaded functions no longer have a negative side effect on here documents.

BZ#651888

Previously, ksh did not restore file handles after executing a sourced script. If an output stream or an

error stream was redirected in the sourced script, the respective stream remained redirected in the parent script as well. With this update, file handles are restored after execution of sourced scripts so a parent script is not affected by sourced script redirections.

BZ#660319

Previously, a ( ) compound list did not always use a copy of the environment which caused the original environment to be altered. Scripts could behave unexpectedly because their variables could be changed. With this update, a copy of the environment is always used for a ( ) compound list; thus, the original environment is not affected by commands from the ( ) compound list.

Ehnahcements

BZ#582690

The ksh built-in "ulimit" command now provides the ability to read and set the "RLIMIT_RTPRIO" and "RLIMIT_NICE" resource limiters.

BZ#659658

The ksh package now includes an "alternatives" command which allows ksh to be switched with mksh (MirBSD Korn Shell). This enhancement allows users to switch between the ksh-93 and ksh-88 (provided by mksh) shells and to port ksh-88 scripts to ksh-93.

Users are advised to upgrade to this updated ksh package, which resolves these issues and adds these enhancements.

1.169. mod_nss

1.169.1. RHBA-2011:0735 — mod_nss bug fix update

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

The mod_nss module provides strong cryptography for the Apache HTTP Server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

Bug Fixes

BZ#677700

During the Apache HTTP Server startup, a race condition could prevent one or more child processes from receiving the token PIN, rendering such processes unable to use SSL. With this update, the race condition no longer occurs, and all child processes of the Apache HTTP Server can enable SSL as expected.

BZ#682326

Due to an incorrect use of the memcpy() function in the mod_nss module, running the Apache HTTP Server with this module enabled could cause some requests to fail with the following message written to the error_log file:

request failed: error reading the headers

This update applies a patch to ensure that the memcpy() function is now used in accordance with the current specification, and using the mod_nss module no longer causes HTTP requests to fail.

BZ#634687

Under certain circumstances, a large "POST" request could cause the mod_nss module to enter an infinite loop. With this update, the underlying source code has been adapted to address this issue, and mod_nss now works as expected.

BZ#605376

The mod_nss module is shipped with the gencert utility that generates the default NSS database. Prior to this update, this utility was installed without any documentation on its usage. This error has been fixed, and a manual page for gencert is now included as expected.

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

1.170. mutt

1.170.1. RHSA-2011:0959 — Moderate: mutt security update

An updated mutt 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.

Mutt is a text-mode mail user agent.

Security Fix

CVE-2011-1429

A flaw was found in the way Mutt verified SSL certificates. When a server presented an SSL certificate chain, Mutt could ignore a server hostname check failure. A remote attacker able to get a certificate from a trusted Certificate Authority could use this flaw to trick Mutt into accepting a certificate issued for a different hostname, and perform man-in-the-middle attacks against Mutt's SSL connections.

All Mutt users should upgrade to this updated package, which contains a backported patch to correct this issue. All running instances of Mutt must be restarted for this update to take effect.

1.171. net-snmp

1.171.1. RHBA-2011:0729 — net-snmp bug fix update

Updated net-snmp packages that resolve several issues are now available for Red Hat Enterprise Linux 6.

SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps and a version of the netstat command which uses SNMP. This package contains the snmpd and snmptrapd daemons, documentation, etc.

Bug Fixes

BZ#616336, BZ#616764

The IP-MIB::ipAddressTable did not support SNMP SET operation, which enables adding or deleting rows in the IP address table. As a result IPv4 or IPv6 addresses on interfaces could neither be created or removed. The updated packages enhance IP-MIB::ipAddressTable with these functions as per RFC 4293 mandates.

BZ#621664

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 favour of more meaningful and specific error messages, which are written to the system log only once.

BZ#625262

The SNMP daemon did not properly handle netlink sockets when forking to background and becoming a daemon. It could therefore not process incoming notifications from kernel regarding changes in IP-MIB::ipAddressPrefixTable. The updated package fixes the socket processing to ensure SNMP deamon handles incoming kernel notifications and updates ipAddressPrefixTable in runtime.

BZ#627564

The SNMP daemon did not detect and notify newly added or activated interfaces in IPV6-MIB::627564ipv6IfTable. The updated package properly refreshes the table when new interface appears.

BZ#630157

The implementation of BRIDGE-MIB was enhanced with Virtual LANs (RFC 4363).

BZ#636890

The snmpwalk utility did not perform correct OID comparison and printed additional objects when walking through an OID subtree. The updated package fixed the OID comparison so that snmpwalk prints only the objects from requested subtree.

BZ#641113

The SNMP daemon 'snmpd', returned incorrect value of either "0.1" or 1.3" for sysObjectID. This update fixes the value of this OID so it returns the correct value, "1.3.6.1.4.1.8072.3.2.10".

Enhancements

BZ#657835

The Net-SNMP source RPM package failed to compile on machine incase of a disabled IPv6 networking stack since the built-in test suite requires a working IPv6. The updated package correctly recovers from a disabled IPv6 stack and compiles successfully.

BZ#665053

The problem was that in some cases SNMP daemon 'snmpd', wrongly retyped pointers to integer data when processing SMUX packets resulting in a freeze. The pointer operations were fixed in the updated package to avoid snmpd freeze while processing SMUX packets.

BZ#672595

The snmpd daemon handled incorrectly internal list of SMUX registrations, which could result in snmpd crash when processing SMUX messages. The updated package fixes the list handling and does not crash when processing SMUX messages.

BZ#674757

The snmpd daemon did not properly initialize it's structures for IP-MIB::ipSystemStatsTable and IP-MIB::ipIfStatsTable properly. It returned this error message "looks like a 64bit wrap, but prev!=new" to log if a counter in these tables got larger than 32bits. The updated packages fixes initialization of the tables and ensures that the aforementioned message should not appear in snmpd log.

All users of net-snmp are advised to upgrade to these updated packages, which resolve these issues.

1.171.2. RHBA-2012:1410 — net-snmp bug fix update

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

The net-snmp packages provide a generic client library, a suite of command-line tools, an extensible SNMP agent, Perl modules, and Python modules to use and deploy the Simple Network Management Protocol (SNMP).

Bug Fix

BZ#868176

Previously, the snmpd daemon did not verify the result of reading from a network socket in the SMUX (SNMP multiplexing) module. Consequently, snmpd was sometimes unable to close erroneous SMUX sessions, because it failed to detect some network errors. With this update, the snmpd daemon has been adapted to properly detect errors when reading from a SMUX socket and it now reacts to these errors properly.

Users of net-snmp are advised to upgrade to these updated packages, which fix this bug.

1.172. net-tools

1.172.1. RHBA-2011:0690 — net-tools bug fix update

An updated net-tools package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The net-tools package contains basic networking tools, including ifconfig, netstat, route, and others. Netstat prints information about the Linux networking subsystem.

Bug Fixes

BZ#682368

Unless a device name was specified on the command line, the mii-tool utility automatically checked Ethernet interfaces from eth0 to eth7. Similarly, running the mii-diag or ether-wake utility without the device name caused it to use eth0 by default. However, Red Hat Enterprise Linux 6.1 introduces the possibility to use arbitrary names for these network interfaces. Because of this, the mii-tool, mii-diag, and ether-wake utilities have been adapted to require a device name to be specified on the command line.

BZ#580054

Due to an incorrect use of 32-bit integers, running the netstat utility with the "-s" (or "--statistics") command line option on a 64-bit architecture could cause some entries in the "IpExt" section to be displayed with negative values. With this update, integers on 64-bit architectures are now handled properly, and the "netstat -s" command now produces the correct output.

BZ#634539

When the netstat utility is run with the "-c" (or "--continuous") command line option, it prints the selected information continuously every second. Previously, netstat failed to free the allocated memory. Consequent to this, running the utility for a long time could cause it to consume all available memory. With this update, the underlying source code has been corrected to free the allocated memory when appropriate, and running the netstat utility with the "-c" option no longer leads to a memory leak.

BZ#614931

Prior to this update, the manual page for the netstat utility stated that running the utility with the "-a" (or "--all") command line option allows a user to list both listening and non-listening sockets. Since this description was rather vague, this update extends the manual page to provide a clear explanation of which sockets are classified as non-listening.

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

1.173. netcf

1.173.1. RHBA-2011:0620 — netcf bugfix update

An updated netcf package that fixes various bugs is now available.

Netcf is a library for modifying the network configuration of a system. Network configurations are expressed in a platform-independent XML format, which netcf translates into changes to the system's 'native' network configuration files.

This update rebases netcf from version 0.1.6 to the current upstream version, 0.1.7. (BZ#651032)

This rebase addresses several issues, including:

BZ#633346

Tight coupling between netcf and gnulib

* Disallowing firewall rules editing

* An iptables rule tweak regarding tuneable kernel necessity

This re-base also incorporates fixes for two bugs as follows:

* Previously, after a reboot, virInterface functions did not work until libvirt was restarted and instead failed with a "error: Failed to list active interfaces. error: this function is not supported by the connection driver: virConnectNumOfInterfaces" error message. This is now fixed so that the code that caused the problem is removed and virInterface functions operate as expected after a reboot.

BZ#629206

Previously, netcf was unable to initialize due to the system's iptables configuration and failed with a "Failed to initialize netcf. error: unspecified error" error message. This is now fixed and netcf no longer fails during initialization.

Users are advised to upgrade to this updated package, which resolves these issues.

1.174. netlabel_tools

1.174.1. RHBA-2011:0191 — netlabel_tools bug fix update

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

NetLabel is a kernel subsystem which implements explicit packet labeling protocols such as CIPSO and RIPSO for Linux. Packet labeling is used in secure networks to mark packets with the security attributes of the data they contain. This package provides the necessary user space tools to query and configure the kernel subsystem.

Bug Fix

BZ#602291

Previously, running the netlabelctl utility with an invalid mask argument caused the utility to terminate with a 0 exit status. This error has been fixed, and when an invalid mask is supplied, netlabelctl now returns a non-zero exit status as expected.

All users of netlabel_tools are advised to upgrade to this updated package, which resolves this issue.

1.175. NetworkManager

1.175.1. RHSA-2011:0930 — Moderate: NetworkManager security update

Updated NetworkManager 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.

NetworkManager is a network link manager that attempts to keep a wired or wireless network connection active at all times.

Security Fix

CVE-2011-2176

It was found that NetworkManager did not properly enforce PolicyKit settings controlling the permissions to configure wireless network sharing. A local, unprivileged user could use this flaw to bypass intended PolicyKit restrictions, allowing them to enable wireless network sharing.

Users of NetworkManager should upgrade to these updated packages, which contain a backported patch to correct this issue. Running instances of NetworkManager must be restarted ("service NetworkManager restart") for this update to take effect.

1.175.2. RHSA-2011:1338 — Moderate: NetworkManager security update

Updated NetworkManager 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.

NetworkManager is a network link manager that attempts to keep a wired or wireless network connection active at all times. The ifcfg-rh NetworkManager plug-in is used in Red Hat Enterprise Linux distributions to read and write configuration information from the /etc/sysconfig/network-scripts/ifcfg-* files.

Security Fix

CVE-2011-3364

An input sanitization flaw was found in the way the ifcfg-rh NetworkManager plug-in escaped network connection names containing special characters. If PolicyKit was configured to allow local, unprivileged users to create and save new network connections, they could create a connection with a specially-crafted name, leading to the escalation of their privileges. Note: By default, PolicyKit prevents unprivileged users from creating and saving network connections.

Red Hat would like to thank Matt McCutchen for reporting this issue.

Users of NetworkManager should upgrade to these updated packages, which contain a backported patch to correct this issue. Running instances of NetworkManager must be restarted ("service NetworkManager restart") for this update to take effect.

1.175.3. RHBA-2011:0769 — NetworkManager bug fix and enhancement update

Updated NetworkManager packages that fix a number of bugs and add some enhancements are now available.

NetworkManager is a system network service that manages network devices and connections, attempting to keep active network connectivity when available. It manages Ethernet, wireless, mobile broadband (WWAN), and PPPoE devices, and provides VPN integration with a variety of different VPN services.

Bug Fixes

BZ#584271

After Wireless was disabled in NetworkManager, a suspend and resume operation caused the wireless connection to become enabled automatically. This is now fixed to preserve the user set wireless state even after an rfkill operation (suspend and resume).

BZ#589230

Translations had assorted inconsistencies, including invalid characters as part of the network-manager-applet (languages: as, te, pa, gu, mr, fr, es, bn_IN) and NetworkManager (languages: bn_IN, es, fr, ja, mr). These are now fixed to display the correct translated strings.

BZ#608663

Due to a type truncation problem on 64-bit PPC systems, correctly configured connections was not displayed in connection editor. This is now fixed and connections are properly shown in the editor on all platforms as expected.

BZ#626337

Unprivileged users could change the status of the wireless connection and WWAN. This is now fixed to display a "not authorized" error for any unauthorized users attempting to change the wireless status.

BZ#627649

NetworkManager would insert warning messages in the /var/log/messages log file due to the hostname operation. This is now fixed to ensure no unnecessary warnings display during the hostname operation.

BZ#633501

Occasionally, the NetworkManager panel applet would not be able to determine user permissions to enable networking and therefore disabled the "Enable Networking" and "Enable Wireless" check boxes. This is now fixed to ensure that if the user has permissions to enable networking, the check boxes display as expected.

BZ#636877

Roaming between WPA/WPA2 access points in the same SSID attached to the same wireless LAN controller resulted in an unexpected re-authentication requirement. This is now fixed so that the SSID is preserved to be used again after a legitimate roaming disconnection event.

BZ#666078

Configurations that used multiple network devices where one device was an iSCSI adapter that should not have the default route were incorrectly handled. This is now fixed to ensure that iSCSI devices that are denied the default route do not receive it. (BZ665027)

* IPv6 static addressing configurations were unable to correctly save the gateway address. This is now fixed to ensure that the gateway address now saves the first configured IPv6 address.

BZ#668830

NetworkManager used to update /etc/hosts file, which could cause problems in some configurations. This is now fixed and NetworkManager does not modify /etc/hosts, leaving it for the administrator to set up.

BZ#692578

NetworkManager saved the WPA/WPA2 password despite selecting the "Ask for this password every time" option and presented a password field with some text when prompting the user to enter a new WPA/WPA2 connection password. This is fixed so that NetworkManager does not store passwords when "Ask for this password every time" is selected and displays an empty password field when prompting the user for the password.

Enhancements

BZ#634152

IPv6 information such as the IP Address and DNS servers now displays in the connection information.

BZ#662730

DHCP lease change events now trigger dispatcher scripts at the /etc/NetworkManager/dispatcher.d location.

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

1.176. NetworkManager-openswan

1.176.1. RHBA-2011:0746 — NetworkManager-openswan bug fix update

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

NetworkManager-openswan contains software for integrating the Openswan VPN software with NetworkManager and the GNOME desktop.

Bug Fix

BZ#659709

Previously, it took as much as 45 seconds for NetworkManager-openswan to time out when an incorrect password or incorrect group secret was given. With this update, a fix has been provided and NetworkManager-openswan now fails immediately upon bad credentials.

Users of NetworkManager-openswan are advised to upgrade to this updated package, which fixes this bug.

1.177. nfs-utils

1.177.1. RHBA-2011:0738 — nfs-utils bug fix and enhancement update

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

The nfs-utils package provides a daemon for the kernel Network File System (NFS) server, and related tools such as the mount.nfs, umount.nfs, and showmount programs.

Bug Fixes

BZ#625080

The "nfsstat --nfs" command did not return any results for NFS version 4 clients because the has_stats() function did not support statistics for the NFS version 4 clients. This update adapts the underlying code and the command returns the values as expected.

BZ#628996

Previously, running the rpc.nfsd program as the root user caused a kernel panic due to a NULL pointer dereference in the nfsd_svc() function. This update applies a number of fixes to the nfsd daemon, which fixes the bug.

BZ#631012

Previously, mounting NFS over RDMA (remote direct memory access) failed due to missing code for such mounting in the NFS initialization script and the sysconfig file. This update adds the missing code and mounting of NFS over RDMA works correctly.

BZ#636513

On shutdown, nfs-utils failed to unmount the /var/ file system correctly because the name of the

subsystem lock file did not match the name of the lock file nfs-utils was searching for. This update changes the name of the lock file so that the shutdown script locates the file and unmounts the file system successfully.

BZ#641291

Previously, servers configured to use only the NFS version 4 (NFSv4) services could have failed to start. This occurred because the /etc/sysconf/nfs configuration file defined the MOUNTD_NFS_V1 option, which is no longer supported. This update removes the variable from the configuration file and servers using NFSv4 start as expected.

BZ#663153

Previously, the %pre scriptlet called the "groupadd" command with an invalid command line argument during package installation. With this update, the command uses the correct argument.

BZ#698220

Previously, an incorrect principal in the NFS client request could have caused the rpc.svcgssd daemon to terminate unexpectedly with a segmentation fault. This was caused by an error in the underlying code. This update adapts the code and rpc.svcgssd no longer crashes.

Enhancements

BZ#637198

This update adds IPv6 (Internet Protocol version 6) support for the server.

BZ#671474

Prior to this update, nfs-utils tried to construct the principal name for the local host and attempted to match it against entries in the keytab file to acquire a Ticket Granting Ticket (TGT). With this update, nfs-utils opens the file and picks the appropriate name from the list of principals so that the NFS client machine is able to authenticate even after its host name is changed.

Users are advised to upgrade to this updated nfs-utils package, which resolves these issues and adds these enhancements.

1.177.2. RHBA-2012:0671 — nfs-utils bug fix update

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

The nfs-utils packages provide a daemon for the kernel Network File System (NFS) server and related tools, which provides better performance than the traditional Linux NFS server used by most users. These packages also contain the mount.nfs, umount.nfs, and showmount programs.

Bug Fix

BZ#812448

Previously, the nfsd daemon was started before the mountd daemon. However, nfsd uses mountd to validate file handles. Therefore, if an existing NFS client sent requests to the NFS server when nfsd was started, the client received the ESTALE error causing client applications to fail. This update changes the startup order of the daemons: the mountd daemon is now started first so that it can be correctly used by nfsd, and the client no longer receives the ESTALE error in this scenario.

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

1.177.3. RHBA-2011:1397 — nfs-utils bug fix update

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

The nfs-utils package provides a daemon for the kernel Network File System (NFS) server and related tools, which provides better performance than the traditional Linux NFS server used by most users. This package also contains the mount.nfs, umount.nfs, and showmount programs.

Bug Fix

BZ#731309

Previously, the function responsible for parsing the /proc/mounts file was not able to handle single quote characters in the path name of a mount points entries. As a consequence, an NFS exported file system could not be unmounted if its mount point contained space characters. To fix this problem, the parsing routine has been rewritten so that it now parses entries in the /proc/mounts file properly. All NFS file systems now can be unmounted as expected.

All users of nfs-utils are advised to upgrade to this updated package, which fixes this bug.

1.178. nfs-utils-lib

1.178.1. RHBA-2011:0732 — nfs-utils-lib bug fix update

Updated nfs-utils-lib packages that fix several bugs are now available.

The nfs-utils-lib package contains support libraries required by programs in the nfs-utils package.

Bug Fixes

BZ#650970

A number of warnings from librpcsecgss and libnfsidmap were printed unnecessarily while attempting to build nfs-utils-lib. These superfluous warnings have been removed.

BZ#650997

Default values for nfs-utils-lib were not set correctly in the /etc/idconf.conf file. This resulted in default values not being correct on Red Hat Enterprise Linux 6. The configuration has been corrected and now provides sensible defaults.

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

1.179. nspr

1.179.1. RHBA-2011:0692 — nspr bug fix and enhancement update

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

Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing, calendar time, basic memory management (malloc and free), and shared library linking.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSLv2, SSLv3, TLS, and other security standards.

The nss, nss-softokn, and nss-utilpackage packages have been upgraded to upstream version 3.12.9, which provides a number of bug fixes and enhancements over the previous version. (BZ#668055)

Bug Fixes

BZ#555825

Prior to this update, the softokn **PKCS#11** module interface used a wrong object type which caused it to return an object with an invalid ***CKA_CERTIFICATE_TYPE*** attribute. With this update, the softokn **PKCS#11** module interface uses the correct object type.

BZ#589636

Rebuilding the nss package when **IPv6** is enabled caused it to enter a loop in the test part of the rebuild. With this update, the **selfserv** test tool has been modified to use a dual-stack IPv6 listening socket, which can accept connections from both IPv4 and IPv6 clients.

BZ#602629

The help page displayed after issuing the **certutil -H** command was missing the **-W** option (which changes the password to a key database). With this update, the **-W** option has been added to the help page.

BZ#630101

Importing a private key (using the **pk12util** command) did not work for private keys placed in the **/etc/pki/nssdb/** directory due to permission restrictions. This update addresses this issue, and the **nss-sysinit** module now enables the root user to import private key.

BZ#630103

Due to a bug in the nss-sysinit package, visiting a specific website in the Mozilla Firefox web browser caused that website to return an **This Connection is Untrusted.** error even though the web page had a valid security certificate. With this update, this issue has been fixed and visiting the specific web site no longer returns SSL errors.

BZ#631000

Prior to this update, **PKCS#8** encoded PEM (Privacy Enhanced Mail) RSA private key files could not be read by **nss** and resulted in an error when being imported. With this update, **nss** correctly handles the aforementioned files.

BZ#631586

This update fixes an unclosed comment in the source code which occurred after the said comment was reduced to a one line comment by a previously applied patch.

BZ#637948

Support for Intel Advanced Encryption Standard Instructions (AES-NI) in the nss package has been enabled and works as expected.

BZ#642767

This update fixes possible memory leaks in the **`SECKEY_DestroyPublicKey(SECKEY_ImportDERPublicKey(…))`** function.

BZ#643134

Under certain circumstances, after removing a Certificate Authority (CA) from the trust database, **nss** continues to consider the removed CA as trusted. This was due to improper handling of trust flags when removing a CA from the trust database. With this update, trust flags from the user database take precedence over the trust flags inherited from the system database, fixing this issue.

BZ#643553

Prior to this update, when the **setup-nsssysinit.sh** script rewrote/recreated the **`pkcs11.txt`** file, it took the current **`umask`** (user mask) into an account. However, if run with restrictive **`umask`** settings, the **`pkcs11.txt`** file could be created with permissions that did not allow non-privileged users to read it. This could cause **nss-sysinit** to remain disabled even when it was intended to be enabled. With this update, the permissions of the **`pkcs11.txt`** file are changed at the end of the run of the **setup-nsssysinit.sh** script, fixing this issue.

BZ#647834

The **`%verify(not md5 size mtime)`** declarations have been added to the configuration files.

BZ#643554

The **nss-sysinit** application is no longer disabled after the package is upgraded.

BZ#643564

Issuing an **`OpenLDAP`** command and using the LDAPTLS_CACERTDIR variable to pass in an arbitrary directory containing other directories caused the command to abort because OpenLDAP tried to pass down the directory as a file. With this update, specified files that are directories are properly rejected in the aforementioned case.

BZ#656697

The **`PayPalEE.cert`** certificate expired on Oct 31, 2010, which caused thenss package to fail to build. This update prolongs this expiration date of this certificate, and the nss package no longer fails to build.

BZ#676387

Various headers have been added to the nss-softokn-freebl-devel subpackage.

BZ#694663

Updating the nss package but not the curl package on systems configured with both Satellite and non-Satellite repositories resulted in a segmentation fault in **Yum**. With this update, the segmentation fault no longer occurs in the aforementioned case.

Ehnancemets

BZ#642342

The nss package has been updated for the 3.6.11 version of Mozilla Firefox.

BZ#643556

This update introduces **nss-sysinit** status reporting.

BZ#689031

This update enables nss to use PEM files interchangeably in a single process.

All users of nspr, nss, nss-softokn, and nss-util are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.180. nss

1.180.1. RHSA-2011:1282 — Important: nss and nspr security update

Updated nss and nspr 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 cross-platform development of security-enabled client and server applications.

Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.

Security Fix
It was found that a Certificate Authority (CA) issued fraudulent HTTPS certificates. This update renders any HTTPS certificates signed by that CA as untrusted. This covers all uses of the certificates, including SSL, S/MIME, and code signing. (BZ#734316)

Note: This fix only applies to applications using the NSS Builtin Object Token. It does not render the certificates untrusted for applications that use the NSS library, but do not use the NSS Builtin Object Token.

These updated packages upgrade NSS to version 3.12.10 on Red Hat Enterprise Linux 4 and 5. As well, they upgrade NSPR to version 4.8.8 on Red Hat Enterprise Linux 4 and 5, as required by the NSS update. The packages for Red Hat Enterprise Linux 6 include a backported patch.

All NSS and NSPR users should upgrade to these updated packages, which correct this issue. After installing the update, applications using NSS and NSPR must be restarted for the changes to take effect.

1.180.2. RHSA-2011:1444 — Important: nss security and bug fix 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.

It was found that the Malaysia-based Digicert Sdn. Bhd. subordinate Certificate Authority (CA) issued HTTPS certificates with weak keys. This update renders any HTTPS certificates signed by that CA as untrusted. This covers all uses of the certificates, including SSL, S/MIME, and code signing. Note: Digicert Sdn. Bhd. is not the same company as found at digicert.com. (BZ#751366)

Note: This fix only applies to applications using the NSS Builtin Object Token. It does not render the certificates untrusted for applications that use the NSS library, but do not use the NSS Builtin Object Token.

This update also fixes the following bug on Red Hat Enterprise Linux 5:

BZ#743508

When using mod_nss with the Apache HTTP Server, a bug in NSS on Red Hat Enterprise Linux 5 resulted in file descriptors leaking each time the Apache HTTP Server was restarted with the "service httpd reload" command. This could have prevented the Apache HTTP Server from functioning properly if all available file descriptors were consumed.

For Red Hat Enterprise Linux 6, these updated packages upgrade NSS to version 3.12.10. As well, they upgrade NSPR (Netscape Portable Runtime) to version 4.8.8 and nss-util to version 3.12.10 on Red Hat Enterprise Linux 6, as required by the NSS update. (BZ#735972, BZ#736272, BZ#735973)

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. In addition, on Red Hat Enterprise Linux 6, applications using NSPR and nss-util must also be restarted.

1.181. nss-pam-ldapd

1.181.1. RHBA-2011:0796 — nss-pam-ldapd bug fix update

An updated nss-pam-ldapd package is now available for Red Hat Enterprise Linux 6.

The nss-pam-ldapd provides the nss-pam-ldapd daemon (nslcd) which uses a directory server to look up name service information on behalf of a lightweight nsswitch module.

Bug Fixes

BZ#690870

Prior to this update, nslcd did not allow parentheses to be used in a valid name. With this update, the implementation of the "validusers" configuration option has been added and the use of opening and closing parentheses in usernames and groupnames is now allowed.

BZ#692225

Verifying the nss-pam-ldapd package (by executing the "rpm --verify nss-pam-ldapd" command) failed in the /etc/nslcd.conf file due to changes in that configuration file performed after the installation of the package. With this update, post-installation changes in the /etc/nslcd.conf file no longer affect the verification of the nss-pam-ldapd package.

BZ#692496

The nslcd man page syntax contained an error which caused the man page to return the following error message on the standard error output:

Error parsing *roff command from file /usr/share/man/man8/nslcd.8.gz

This update fixes the syntax error and the "man nslcd" command no longer returns an error message.

BZ#692817

When nslcd was configured to use multiple LDAP servers, it failed to fall back to a different server in case the primary server could not be reached. This was due to nslcd trying to keep the first

connection alive even when the connection was dropped. With this update, nslcd correctly falls back to a different server after loosing connection with the current one.

All users of nss-pam-ldapd are advised to upgrade to this updated package, which resolves these issues.

1.182. nss-softokn

1.182.1. RHBA-2011:1844 — nss-softokn bug fix update

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

Network Security Services (NSS) is a set of libraries designed to support the development of security-enabled client and server applications. The nss-softokn packages provide NSS Softoken Cryptographic Module.

Bug Fix

BZ#716532

On a 64-bit CPU with native AES instruction support, the intel_aes_decrypt_cbc_256() function did not work correctly when input and output buffers were the same and the function call failed with the message "data mismatch". This update fixes the code and the same buffer can be used for input and output.

All users of nss-softokn are advised to upgrade to these updated packages, which fix this bug. After installing the update, applications using NSS must be restarted for the changes to take effect.

1.183. nss_db

1.183.1. RHBA-2011:0942 — nss_db bug fix update

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

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#718203

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.

1.184. oddjob

1.184.1. RHBA-2011:0339 — oddjob bug fix update

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

The oddjobd service runs specified privileged tasks for unprivileged client applications which communicate with it through the system message bus.

Bug Fixes

BZ#634356

Previously, the oddjobd service failed to reconnect to the system message bus after it lost its connection due to an internal function call. With this update, the oddjobd service is now able to reconnect to the message bus successfully after it loses a connection.

BZ#678345

If a umask is not specified in the oddjobd service's configuration file, the service now uses the UMASK setting, if present, to calculate the permissions which should be set on a user's home directory.

BZ#664418

The oddjobd service did not ensure, when creating a user's home directory, that any intermediate directories that were created would have correct permissions. This could have caused users to be unable to access their home directory. With this update, oddjobd ensures that correct permissions are set for any intervening directories such that the user is able to access their home directory.

BZ#674534

The oddjobd init script exited with a exit status of "1" when it was passed a non-existent action. Service init scripts should exit with an exit code of "2" when they are asked to perform an unknown action. The oddjobd init script has been corrected, and now conforms with init script guidelines.

BZ#659681

The oddjobd service failed to register the name of the mkhomedir service because the message bus was not signaled to re-read its configuration files when the oddjob-mkhomedir package was installed. With this update, oddjobd is now able to register the mkhomedir service name successfully.

All oddjobd service users are advised to upgrade to these updated packages which fix these bugs.

1.185. openais

1.185.1. RHBA-2011:0740 — openais bug fix update

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

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais packages contain the OpenAIS service handlers and default configuration files.

Bug Fix

BZ#630110

Previous versions of the openais packages included the /etc/rc.d/init.d/openais init script with the stop priority set to "20". Consequent to this, shutting down a system caused this init script to stop the

openais service in a wrong order. Since this init script is not needed, this update removes /etc/rc.d/init.d/openais from the packages, and the openais service is now stopped when expected.

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

1.186. opencryptoki

1.186.1. RHBA-2011:0661 — opencryptoki bug fix and enhancement update

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

The openCryptoki package contains version 2.11 of the PKCS#11 API, implemented for IBM Cryptocards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded), the IBM eServer Cryptographic Accelerator (FC 4960 on IBM eServer System p), the IBM Crypto Express2 (FC 0863 or FC 0870 on IBM System z), and the IBM CP Assist for Cryptographic Function (FC 3863 on IBM System z).

The openCryptoki package has been upgraded to upstream version 2.3.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#632765)

Bug Fixes

BZ#604287

Previously, openCryptoki failed to include secure key support on IBM System z. This was caused by an incorrect build configuration. This update provides the package built with the correct configuration and adds secure key support for System z to the package.

BZ#654088

Prior to this update, openCryptoki failed with the CKR_FUNCTION_FAILED error when trying to sign a certificate for an NSS (Network Security Services) database. This occurred due to the function being called incorrectly. With this update, openCryptoki uses the correct function arguments and the error no longer occurs.

Users of opencryptoki are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.186.2. RHBA-2011:1389 — opencryptoki bug fix update

Updated opencryptoki packages that fix one bug are now available For Red Hat Enterprise linux 6.

The opencryptoki package contains version 2.11 of the PKCS#11 API, implemented for IBM Cryptocards, such as IBM 4764 and 4765 crypto cards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded), the IBM eServer Cryptographic Accelerator (FC 4960 on IBM eServer System p), the IBM Crypto Express2 (FC 0863 or FC 0870 on IBM System z), and the IBM CP Assist for Cryptographic Function (FC 3863 on IBM System z). The opencryptoki package also brings a software token implementation that can be used without any cryptographic hardware. This package contains the Slot Daemon (pkcsslotd) and general utilities.

Bug Fix

BZ#743556

When setting the length of an RSA key for the IBM Cryptographic Accelerator(ICA) token, initialization of the CKA_MODULUS_BITS internal attribute of PKCS#11 was not properly tested and the RSA key length could have been set incorrectly. As a consequence, RSA key verification in the ICA token failed. To ensure that the RSA key is set correctly, two conditions have been added in the respective function in the ICA specific library. The RSA key operations now work properly on the ICA token.

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

1.187. openldap

1.187.1. RHBA-2011:0673 — openldap bug fix and enhancement update

Updated openldap packages that fix several bugs and add an enhancement are now available.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

Bug Fixes

BZ#548475

Move openldap libraries from /usr/lib to /lib.

BZ#613966

Init script is working wrong if database recovery is needed.

BZ#630637

Update list of modules in slapd.conf.bak.

BZ#644399

slapd init script gets stuck in an infinite loop.

BZ#685119

openldap-servers upgrade hangs or do not upgrade the database

Users are advised to upgrade to these packages, which resolve these issues.

1.187.2. RHBA-2012:0453 — openldap bug fix update

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

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

Bug Fixes

BZ#790913

Mozilla NSS initialization functions are not implemented in a thread-safe way. Therefore, if multiple TLS operations were performed simultaneously on an LDAP server, a race condition between the TLS threads could occur. Consequently, the LDAP server terminated unexpectedly with a segmentation fault. With this update, a mutual exclusion (mutex) for Mozilla NSS initialization functions calls has been added to the code, which prevents this situation from occurring. The LDAP server no longer crashes when initializing a TLS connection.

BZ#790914

Previously, OpenLDAP used incorrect data types for storing the length of the values used by the ODBC (Open Database Connectivity) interface in the SQL back end implementation. As a consequence, the LDAP server terminated unexpectedly with a segmentation fault after a few operations. This update modifies the code to use the correct data types so that the LDAP server no longer crashes when using the SQL back end.

BZ#790915

Previously, OpenLDAP did not properly handle wildcarded common names (for example CN=*.example.com) in LDAP certificates. Therefore, when a program used OpenLDAP for a secure SSL/TLS connection to an LDAP server using an LDAP certificate with a wildcarded common name, the connection failed. With this update, the code of OpenLDAP has been modified to properly test common names in LDAP certificates so that a connection to the LDAP server now succeeds if the wildcarded common name matches the server hostname.

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

1.187.3. RHEA-2011:1335 — openldap enhancement update

Enhanced openldap packages are now available for Red Hat Enterprise Linux 6.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. The openldap packages contain configuration files, libraries, and documentation for OpenLDAP.

Enhancement

BZ#733659

In a distributed environment, a Root DN (distinguished name) can be specified instead of a hostname to connect to an OpenLDAP server. The Root DN is used to look up the corresponding hosts using the DNS SRV (Domain Name Server Service) records. Prior to this update, the priority and weight of individual SRV records were ignored and the connection was created to the host in the first SRV record returned by the DNS server. As a consequence, a server in a different geographic location may have been queried, leading to high response times. Servers are now queried according to their priority and weight, which conforms to the RFC 2782 standard.

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

1.187.4. RHBA-2011:1124 — openldap bug fix update

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

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. The openldap packages contain configuration files, libraries, and documentation for OpenLDAP.

Bug Fix

BZ#723134

Prior to this update, client certificates were under certain circumstances not released when OpenLDAP validated the Transport Layer Security (TLS) peer and the client certificate was cached by Mozilla NSS library. Due to this problem, tools that used both OpenLDAP and Mozilla NSS libraries could fail when calling the NSS_Shutdown function. This update releases the certificate in the OpenLDAP library after finishing the validation. Now, all caches can be released and NSS_Shutdown succeeds.

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

1.188. openmpi

1.188.1. RHEA-2011:0590 — openmpi bug fix and enhancement update

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

Open MPI is the Open Message Passing Interface software stack used for cluster communications in High Performance Compute clusters.

Enhancement

BZ#632371

The OpenMPI packages have been upgraded to upstream version 1.4.3, which provides a number of bug fixes and enhancements.

Bug Fix

BZ#661292

Previously, the line "BuildRequires: flex" was missing in the spec file. This caused the package build to fail unless flex was manually installed. This update adds the line to the spec file.

All users of Open MPI are advised to upgrade to these updated openmpi packages, which fix this bug and add this enhancement.

1.189. openscap

1.189.1. RHBA-2011:0609 — openscap bug fix and enhancement update

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

The Security Content Automation Protocol (SCAP) is a line of standards that provide a standard language for the expression of Computer Network Defense related information. OpenSCAP is a set of open source libraries for the integration of SCAP.

The openscap packages have been upgraded to upstream version 0.7.1, which provides a number of bug fixes and enhancements over the previous version. The most important changes include support for Open Vulnerability and Assessment Language (OVAL) version 5.6, the new OpenSCAP API, and various memory and CPU optimizations. (BZ#642672)

Bug Fix

BZ#669693

Previously, sending the "USR1" signal to all probes in order to abort the execution of a current rule could cause the oscap utility to stop responding or even terminate unexpectedly with a segmentation fault. This update adapts the underlying source code to prevent such behavior, and when the "USR1" signal is received, the oscap utility now correctly aborts the execution of the selected rule and continues with the remaining rules as expected.

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

1.190. openssh

1.190.1. RHBA-2011:0598 — openssh bug fix and enhancement update

Updated openssh packages that fix several bugs and add various enhancements 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#631757

When the ~/.bashrc startup file contained a command that produced output to standard error, the sftp utility was unable to log in to the user account. This bug has been fixed, and output to standard error is discarded and no longer prevents the sftp utility from establishing the connection.

BZ#631787

Due to the limitations of the data type that was used to store user identifier (UID) numbers, the lastlog record was not created for a user with a UID larger than 2147483647. With this update, this data type has been changed to unsigned long integer, and the /var/log/lastlog database is now updated as expected.

BZ#646286

Previously, GSSAPI key exchange functionality was not supported. With this update, GSSAPI key exchange is now supported and works as expected.

BZ#652249

Previously, the openssh package did not contain the **`README.nss`** file. This update adds the file to the documentation.

BZ#656415

Logging in to a system caused pam_ssh_agent_auth to temporarily set the EUID (Effective User ID) to the user's current UID. However, if the connection failed, the original EUID was not restored. This update corrects this coding error so that the EUID is restored in this situaton.

BZ#656844

Previously, openssh could have terminated with a segmentation fault if used as a SOCKS proxy. This occurred due to an unhandled null pointer. With this update the underlying code has been fixed and the problem no longer occurs.

BZ#670515

Previously, the ssh-keygen(1) manual page did not document the "-n" option. This update adds the option description to the manual page.

BZ#672870

Previously, the sshd daemon could have failed to start on a server in FIPS (Federal Information Processing Standards) mode. This happened because the daemon expected an RSA1 server key to be created on startup and checked if the key was available. However, in FIPS mode, no RSA1 key is generated on startup. With this update, the underlying code has been changed and the check is no longer performed when in FIPS mode.

BZ#676665

Previously, the sshd daemon could have failed to locate an authorized key if both MLS (Multi-Level Security) SELinux policy and polyinstantiation of home directories were enabled. This occurred because the daemon was searching for authorized keys in the wrong home directories. This update adds the ssh-keycat helper program, which locates and passes the keys to sshd.

BZ#681296

By default, OpenSSH utilities use the /dev/urandom random number generator (RNG). This update adds the "SSH_USE_STRONG_RNG" environment variable. Setting "SSH_USE_STRONG_RNG=1" (the recommended location to set this environment variable is in the /etc/sysconfig/sshd configuration file) causes OpenSSH utilities to use the stronger /dev/random RNG, which is better at ensuring the RNG always has sufficient entropy.

NOTE

Setting "SSH_USE_STRONG_RNG=1" is resource-intensive, and should generally only be done on servers which have a hardware-enabled random number generator.

BZ#690127

Prior to this update, the openssh-keycat subpackage was optional and OpenSSH thus failed to meet Common Criteria. With this update, the package is included in the openssh-server package.

BZ#690391

Previously, if the user sent two SIGHUP signals to the sshd daemon, the daemon terminated unexpectedly. With this update, the underlying code has been changed and the daemon no longer crashes in such circumstances.

Enhancements

BZ#455350

Previously, openssh only allowed users to store their authorized public keys in a local file on each system they wanted to log in to using their private SSH key. With this update, sshd can be configured, using the AuthorizedKeysCommand directive, to extract users' authorized keys from an arbitrary

source using the "external" command. This update also adds the standalone "ssh-ldap-helper" utility, which can be used to extract public keys from an LDAP server. This new functionality thus enables centralized key management.

BZ#642927

The sshd daemon is now built using RELRO protection.

BZ#577998

Previously, the .k5login file was processed on every kerberos authentication. This update adds the KerberosUseKuserok option to the sshd_config file, which allows the user to configure whether user aliases should be verified against the entries in the .k5login file.

BZ#633404

This update adds support for hardware-accelerated encryption modules which are supported by OpenSSL

BZ#642792

Previously, the sshd daemon did not log information regarding logins using key-based authentication to the audit log. With this update, sshd logs the same information that PAM (Pluggable Authentication Modules) logs upon password-based logins, but for key-based logins. Additionally, sshd logs the following additional detail for key-based logins: key type and size, as well as its fingerprint.

BZ#644877

OpenSSH's audit logging support has been updated.

BZ#657059

Previously, the sftp command worked with the default file mode creation mask (umask) only. With this update, the user may change the umask.

BZ#665112

When an authentication key is destroyed, OpenSSH now logs the key destructions to the audit log.

All users of openssh are advised to upgrade to these updated packages, which resolve these issues and provide these enhancements.

1.190.2. RHBA-2011:0848 — openssh bug fix update

Updated openssh packages that fix a bug 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 Fix

BZ#708924

Previously, when the SSH_USE_STRONG_RNG variable was set to 1, openssh read 48 bytes from the /dev/random number generator to generate a seed. This seed was too long and caused long delays on ssh or sshd startup and when connections were received. Now, the SSH_USE_STRONG_RNG variable contains number of bytes that should be pulled from /dev/random (with a minimum default value of six) and the delays no longer occur.

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

1.191. openssl

1.191.1. RHSA-2011:0677 — Moderate: openssl security, bug fix, and enhancement update

Updated openssl packages that fix one security issue, two bugs, and add two enhancements are now available for Red Hat Enterprise Linux 6.

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

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

Security Fix

CVE-2011-0014

A buffer over-read flaw was discovered in the way OpenSSL parsed the Certificate Status Request TLS extensions in ClientHello TLS handshake messages. A remote attacker could possibly use this flaw to crash an SSL server using the affected OpenSSL functionality.

Bug Fixes

BZ#619762

The "openssl speed" command (which provides algorithm speed measurement) failed when openssl was running in FIPS (Federal Information Processing Standards) mode, even if testing of FIPS approved algorithms was requested. FIPS mode disables ciphers and cryptographic hash algorithms that are not approved by the NIST (National Institute of Standards and Technology) standards. With this update, the "openssl speed" command no longer fails.

BZ#673453

The "openssl pkcs12 -export" command failed to export a PKCS#12 file in FIPS mode. The default algorithm for encrypting a certificate in the PKCS#12 file was not FIPS approved and thus did not work. The command now uses a FIPS approved algorithm by default in FIPS mode.

Enhancements

BZ#601612

The "openssl s_server" command, which previously accepted connections only over IPv4, now accepts connections over IPv6.

BZ#673071

For the purpose of allowing certain maintenance commands to be run (such as "rsync"), an "OPENSSL_FIPS_NON_APPROVED_MD5_ALLOW" environment variable has been added. When a system is configured for FIPS mode and is in a maintenance state, this newly added environment variable can be set to allow software that requires the use of an MD5 cryptographic hash algorithm to be run, even though the hash algorithm is not approved by the FIPS-140-2 standard.

Users of OpenSSL are advised to upgrade to these updated packages, which contain backported patches to resolve these issues and add these enhancements. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

1.191.2. RHSA-2011:1409 — 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.

Security Fix

CVE-2011-3207

An uninitialized variable use flaw was found in OpenSSL. This flaw could cause an application using the OpenSSL Certificate Revocation List (CRL) checking functionality to incorrectly accept a CRL that has a nextUpdate date in the past.

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.

1.191.3. RHEA-2011:0868 — openssl enhancement update

Updated openssl packages that adds several enhancements are now available for Red Hat Enterprise Linux 6.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library.

Enhancements

BZ#709020

With this update, the openssl API for the DSA algorithm has been enhanced to allow for presetting the prime (P) and the subprime (Q) parameters when generating the base (G) parameter. This is necessary for the algorithm correctness validation according to the FIPS-186-3 standard.

BZ#711336

With this update, the implementation of the AES encryption algorithm with the support for AES-NI processor instructions is now enabled also in the FIPS mode.

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

1.192. openswan

1.192.1. RHSA-2011:1356 — Moderate: openswan security update

Updated openswan 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.

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.

Security Fix

CVE-2011-3380

A NULL pointer dereference flaw was found in the way Openswan's pluto IKE daemon handled certain error conditions. A remote, unauthenticated attacker could send a specially-crafted IKE packet that would crash the pluto daemon.

Red Hat would like to thank the Openswan project for reporting this issue. Upstream acknowledges Paul Wouters as the original reporter.

All users of openswan are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, the ipsec service will be restarted automatically.

1.192.2. RHSA-2011:1422 — Moderate: openswan security update

Updated openswan 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.

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.

Security Fix

CVE-2011-4073

A use-after-free flaw was found in the way Openswan's pluto IKE daemon used cryptographic helpers. A remote, authenticated attacker could send a specially-crafted IKE packet that would crash the pluto daemon. This issue only affected SMP (symmetric multiprocessing) systems that have the cryptographic helpers enabled. The helpers are disabled by default on Red Hat Enterprise Linux 5, but enabled by default on Red Hat Enterprise Linux 6.

Red Hat would like to thank the Openswan project for reporting this issue. Upstream acknowledges Petar Tsankov, Mohammad Torabi Dashti and David Basin of the information security group at ETH Zurich as the original reporters.

All users of openswan are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, the ipsec service will be restarted automatically.

1.192.3. RHBA-2011:0652 — openswan bug fix and enhancement update

Updated openswan package that fix various bugs and provide several enhancements are now available for Red Hat Enterprise Linux 6.

Openswan is a free implementation of IPsec and IKE (Internet Key Exchange) for Linux. This package contains the daemons and user space tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel.

Openswan 2.6.x also supports IKEv2 (RFC4306)

The openswan packages have been upgraded to upstream version 2.6.32, which provides a number of bug fixes and enhancements over the previous version. (BZ#642724)

Bug Fixes

BZ#621790

Openswan was previously unable to negotiate using the HMAC-SHA2-256 algorithm in transport mode. With this update, Openswan is able to set up IPsec in using HMAC-SHA2-256 in transport mode.

BZ#628879

The Openswan init script accessed the current working directory, which led to an SELinux AVC Denial. This update ensures that the current working directory is set to the root ("/") directory, and thus Openswan's pluto daemon starts without incurring an SELinux denial.

BZ#642722

Previously, the Openswan packages were not compiled with the "-Wl,-z,relro" parameter. These updated openswan packages have been compiled with the "-Wl,-z,relro" parameter.

BZ#658121

The IPsec NETKEY kernel code sent thousands of ACQUIRE messages which led to a segmentation fault. With this update, ACQUIRE messages are now properly processed with the result that Openswan does not crash.

BZ#658253

When the system's IP address was renewed using DHCP, the Openswan IPsec connection failed. This update ensures that the IPsec connection continues to operate across DHCP IP address renewals.

BZ#668785

Entering an incorrect IKE Extended Authentication (Xauth) password during IKE negotiation leads to a failure to connect. However, the failure was not communicated to NetworkManager, with the result that NetworkManager continued to wait for a timeout. With this update, Openswan sends a failure message to NetworkManager over the D-Bus system message bus, informing it of the failure to connect. As a result, NetworkManager knows about the failure as soon as it happens, and is able to inform the user about it immediately.

BZ#681974

Internet Control Message Protocol (ICMP)-specific IPsec connections were set up incorrectly, with incorrect "Type" and "Code" fields, in the code. This has been fixed so that ICMP selectors are now processed correctly according to the IKEv2 protocol specification (RFC 4306).

BZ#683604

Configuring a second IPsec policy using a different host behind the same gateway caused Openswan to crash due to the policy not being set up correctly. With this update, Openswan's IKEv2 implementation processes the traffic selectors correctly so that the correct definition is picked up during the key exchange. As a result, a second IPsec policy using a different host behind the same gateway can successfully set up.

Enhancements

BZ#235720

Openswan's IKEv1 implementation and NETKEY interactions now understand SELinux labeled flows, and Openswan has been integrated with SELinux. As a result, it's now possible to exchange SELinux labels in IKE, and set up labeled IPsec policies and Security Associations (SAs) in SELinux Multi-Level Security (MLS) mode.

BZ#646718

Previously, Openswan did not support the Internet Key Exchange version 2 (IKEv2) USE_TRANSPORT_MODE functionality, with the result that Openswan could not interoperate with racoon2 in transport mode. With this update, Openswan's IKEv2 protocol support has been enhanced so that it now works in transport mode, and interoperate with racoon2.

Users are advised to upgrade to these updated openswan packages, which resolve these issues and add these enhancements.

1.192.4. RHBA-2011:0961 — openswan bug fix update

Updated openswan packages that resolve several issues are now available for Red Hat Enterprise Linux 6.

Openswan is a free implementation of IPsec and IKE (Internet Key Exchange) for Linux. The openswan package contains the daemons and user space tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4306).

Bug Fixes

BZ#712112

Openswan did not handle protocol and port (leftprotoport) configuration correctly if the hostname parameter was configured instead of the ipaddress parameter using Openswan. This update solves this issue, and Openswan now correctly sets up policies with the correct protocol and port even when the hostname parameter is configured.

BZ#712114

Prior to this update, very large security label strings received from the peer were being truncated. The truncated string was then still used. However, this truncated string could, under rare circumstances, turn out to be a valid string, leading to an incorrect policy. Additionally, erroneous queuing of on-demand requests of setting up an IPsec connection was discovered in the IKEv2 (Internet Key Exchange) code. Although not harmful, it was not the intended design. This update fixes both of these issues, and Openswan now correctly handles the IKE setup.

BZ#712168

Previously, Openswan failed to set up AH (Authentication Header) mode security associations (SAs).

This was because Openswan was erroneously processing the AH mode as if it was the ESP (Ecrypted Secure Payload) mode, and was expecting an encryption key. This update fixes this issue, and it is now possible to properly set up AH mode SAs.

BZ#718078

IPsec connections over a loopback interface did not work properly when a specific port was configured. This was because incomplete IPsec policies were being set up, leading to connection failures. This update fixes this issue, and complete policies are now correctly established.

All users of openswan are advised to upgrade to these updated packages, which resolve these issues.

1.193. openwsman

1.193.1. RHBA-2011:0563 — openwsman bugfix update

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

OpenWSMan provides an open-source implementation of the Web Services Management specification (WS-Management) and exposes system management information on the Linux operating system with the WS-Management protocol. WS-Management is based on a suite of web services specifications and usage requirements that exposes a set of operations focused on and covers all system management aspects.

Bug Fixes

BZ#613031

Previously, certain init script return values were incorrect. This update resolves these errors in the code. Now, all return values are correct.

BZ#615922

Previously, the wsman-xml.h, wsman-xml-binding.h and wsman-dispatcher.h header files were missing. With this update, these headers are provided by the libwsman-devel package.

BZ#617549

Previously, the init script did not print an error message if the SSL certificate and the private key were not found. This update checks whether a certificate exists. Now, OpenWSMan closes and prints a message to manually generate a certificate if no certificate was found.

BZ#622793

Previously, OpenWSMan aborted unexpectedly with a segmentation fault when it was started with a debug flag due to a null pointer dereference. This update checks the pointer value. Now, the pointer is no longer dereferenced when its value is null and OpenWSMan runs as expected.

BZ#625160

Previously, OpenWSMan aborted unexpectedly when it was configured in cooperation with Small Footprint CIM Broker (sfcb) and sfcb was stopped. This update corrects this error in the code. Now, the OpenWSMan configuration with sfcb works as expected.

BZ#626773

Previously, the init script was wrongly placed in the /etc/init.d directory. This update corrects this error. Now, the init script is correctly placed in the /etc/rc.d/init.d. directory.

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

1.194. oprofile

1.194.1. RHBA-2011:0566 — oprofile bug fix and enhancement update

An updated oprofile package that fixes one bug and adds two enhancements is now available for Red Hat Enterprise Linux 6.

OProfile is a system-wide profiler for Linux systems. The profiling runs transparently in the background and profile data can be collected at any time. OProfile uses the hardware performance counters provided on many processors, and can use the Real Time Clock (RTC) for profiling on processors without counters.

Bug Fix

BZ#589638

Previously, non-numeric arguments for the opcontrol options which needed numerical arguments (--buffer-size, --buffer-watershed,--cpu-buffer-size, and --callgraph) were written to /dev/oprofile files without any check. Due to this issue, the OProfile profiler accepted negative and non-numeric values. This update adds numeric argument checks for all arguments to opcontrol. Now, OProfile reports illegal non-numeric arguments.

Enhancements

BZ#643478

Previously, the OProfile profiler did not provide the performance monitoring events for the Intel Westmere processor. This update provides the files for the Intel Westmere processor specific performance events and adds code to identify Intel Westmere processors. Now, OProfile provides Intel Westmere specific events.

BZ#650126

Previously, the OProfile profiler did not have events mapping and unit_mask files to describe processor performance events for the new AMD Family 12h, 14h, 15h processors. This update identifies these new processors and provides lists of the available events. Now, OProfile provides support for AMD Family 12h, 14h, 15h processors.

All OProfile users are advised to upgrade to this updated package which fixes this bug and adds these enhancements.

1.195. pacemaker

1.195.1. RHBA-2011:0642 — pacemaker bug fix and enhancement update

Updated pacemaker packages that fix various bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Pacemaker is a high-availability cluster resource manager with a powerful policy engine.

Bug Fixes

BZ#668466

The pacemaker packages have been upgraded to upstream version 1.1.5, which provides a number of bug fixes over the previous version.

BZ#627626

Due to missing Cluster Resource Manager (CRM) scripts, an attempt to run the crm utility caused the following message to be presented to a user:

```
crm_standby not available, check your installation
```

This update re-includes the "crm_master" in the packemaker package, and adapts the crm utility not to require the "crm_standby" and "crm_failcount" scripts, so that the above error message is no longer displayed.

BZ#684825

In a cluster environment managed by both Pacemaker and the CMAN cluster management subsystem, frequent leaving and joining of a node could cause Pacemaker's quorum view to be incorrect. This update applies a patch that addresses this issue, so that the leaving and joining of a node no longer causes Pacemaker's quorum view to be different from CMAN's.

BZ#684838

Previously, rebooting a node in a CMAN managed cluster could cause the fencing daemon to keep the "fenced:default" CPG group on the remaining nodes, leaving the cluster in an inconsistent state. With this update, an upstream patch has been applied to address this issue. As a result, when a node is rebooted and leaves a cluster, the cluster resources correctly run on remaining nodes.

Enhancements

BZ#676286

When using the fence_ipmilan fencing agent, Pacemaker now accepts "diag" as a valid per-device stonith action. With this action enabled, a fenced node receives the "DIAG" signal and creates a dump for diagnostic purposes.

Note that Pacemaker provides the following functionality, and is now the preferred application to perform these tasks:

BZ#310361

Pacemaker provides support for a time-based resource control. This allows system administrators to define the time a resource is down.

BZ#449833

Pacemaker supports time-based resource control. This allows system administrators to define the downtime of individual resources.

BZ#449835

Pacemaker allows users to manually start or stop cluster resources. This enables system administrators to perform maintenance tasks on individual components within a service.

All users of pacemaker are advised to upgrade to these updated packages, which fix these and other bugs, and add this enhancement. Note that pacemaker is considered a Technology Preview in Red Hat Enterprise Linux 6.

1.196. PackageKit

1.196.1. RHBA-2011:0681 — PackageKit bug fix update

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

PackageKit is a D-Bus abstraction layer that allows the session user to manage packages in a secure way using a cross-distribution, cross-architecture API.

Bug Fixes

BZ#617734

Both Mozilla Firefox and the packagekit-plugin included different versions of sqlite in their dependencies. This could cause crashes in Firefox when attempting to use the PackageKit web plug-in to access application icons, since the plug-in attempted to use its version of sqlite to query PkDesktop. This query attempt has been removed, and the web plug-in now works as expected, without crashing Firefox.

BZ#626867

An error message was incorrectly displayed when the cron script packagekit-background.cron was disabled. As this is a configuration option, not an error, the message is no longer displayed in this situation.

BZ#629049

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

BZ#634560

An error in a changelog entry prevented updates to PackageKit. This error has been corrected.

BZ#667923

A critical warning is displayed erroneously when attempting to install a local package with pkcon, the command line PackageKit tool. This warning is no longer displayed erroneously.

BZ#670163

gpk-update-viewer failed to process updates when used in conjunction with yum version 3.2.29 because it attempted to perform the same repository setup twice if the "prerepoconf" attribute was not set. This resulted in an error:

```
    AttributeError: 'PackageKitYumBase' object has no attribute
'prerepoconf'
```

PackageKit logic has now been altered so that this does not occur, and updates are now processed as expected. This issue was discovered and corrected during development, and was not seen in production systems in the field.

Users of PackageKit are advised to upgrade to these updated packages, which resolve these issues.

1.197. pam

1.197.1. RHBA-2011:0685 — pam bug fix and enhancement update

Updated pam packages that fix bugs and add enhancements are now available.

Pluggable Authentication Modules (PAM) provide a system whereby administrators can set up authentication policies without having to recompile programs to handle authentication.

Bug Fixes

BZ#614766

When the pam packages were updated, the /var/log/tallylog and /var/log/faillog files were overwritten with empty files because of an incorrect condition check in the %post script. This has been corrected, and PAM no longer attempts to overwrite tallylog and faillog files when they exist prior to update.

BZ#679069

A code review revealed several small memory leaks and improperly handled error paths in pam_namespace, pam_selinux, pam_limits, pam_pwhistory, pam_time, and pam_group modules. These issues have been corrected.

Enhancements

BZ#622847

The pam_limits module, which sets resource limits for processes, now supports matching individual and ranges of user and group identifiers in its limits.conf configuration file.

BZ#644971

A new pam_faillock module was added to support temporary locking of user accounts in the event of multiple failed authentication attempts. This new module improves functionality over the existing pam_tally2 module, as it also allows temporary locking when the authentication attempts are done over a screen saver.

BZ#677664

The audit records provided by the pam_selinux and pam_tally2 modules have been improved to include tty and remote hostname information in each recorded event.

All pam users are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

1.198. pam_krb5

1.198.1. RHBA-2011:0711 — pam_krb5 bug fix update

An updated pam_krb5 package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The pam_krb5 module allows PAM-aware applications to verify and change user passwords with the help of a KDC.

Bug Fixes

BZ#622938

Previously, pam_krb5 ignored the "verify_ap_req_nofail" configuration setting when it checked whether the credentials from the Key Distribution Center (KDC) were spoofed because of a missing

or otherwise inaccessible local keytab file. Due to this behavior, pam_krb5 wrongly returned a success message. This update reworks the credential verification. Now, the verification settings work as expected.

BZ#690583

Previously, pam_krb5 used a format for password change requests that earlier versions of kadmind could not process. This update uses application programming interfaces (API) that format password change requests which can also be parsed by earlier versions of kadmind.

All pam_krb5 users are advised to upgrade to this updated package, which fixes these bugs.

1.199. pam_ldap

1.199.1. RHBA-2011:0688 — pam_ldap bug fix

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

The pam_ldap module is a Pluggable Authentication Module (PAM) which allows for authentication, authorization and password changes against LDAP servers.

Bug Fixes

BZ#637190

Previously, the password aging policy for users on LDAP servers used a resolution of one day. Due to this issue, users whose password was going to expire in less than a day would not be warned of the impending expiration. This update changes the resolution. Now, a password expiry warning is also shown on the last day when the password expires within the next 24 hours.

BZ#677338

Applications which authenticate multiple users in succession using pam_ldap may leak memory which libraries on which the module depends allocate and initialize when they are loaded. This update marks the module so that it will not be unloaded. Now these libraries and the memory they allocate are no longer lost.

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

1.200. pam_pkcs11

1.200.1. RHBA-2011:0766 — pam_pkcs11 bug fix update

An updated pam_pkcs11 package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The pam_pkcs11 package allows X.509 certificate-based user authentication. It provides access to the certificate and its dedicated private key with an appropriate PKCS (Public Key Cryptographic Standards) #11 module.

Bug Fixes

BZ#586149

The system returned the following debug message to standard error when you logged in with a smart card from the command line and "require smart card login" was enabled:

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

With this update, the message is no longer returned.

BZ#625509

The system returned the following spurious message to standard error when you entered an incorrect personal identification number (PIN) when logging in from the command line with a smart card:

```
ERROR: pam_pkcs11.c:445: open_pkcs11_login() failed: Login
incorrect
```

With this update, only the message "Login incorrect" is displayed and the error details are logged.

All users of pam_pkcs11 are advised to upgrade to this updated package, which resolves these issues.

1.201. papi

1.201.1. RHBA-2011:0783 — papi bug fix and enhancement update

An updated papi package that fixes a bug and provides an enhancement is now available for Red Hat Enterprise Linux 6.

PAPI (Performance Application Programming Interface) is a software library that provides access to the processor's performance-monitoring hardware. This allows developers to track performance-related events, such as cache misses, instructions retired, and clock cycles, to better understand the performance issues of the software.

Bug Fix

BZ#692668

When using PAPI on the AMD family 0x15 processors, the "papi_avail" utility returned that the number of hardware performance counters was four. However, for these processors, the number of hardware performance counters is six. This update implements support for the additional two hardware counters.

Enhancement

BZ#635667

Previously, PAPI did not handle the new event mappings for the AMD Opteron 6000-series processor and some newer AMD family 10h processors. Due to this, PAPI did not recognize or work with these processors. This update adds the lists of the new events and PAPI recognizes and works with the processors correctly.

PAPI users are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

1.202. paps

1.202.1. RHBA-2011:0296 — paps bug fix update

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

The paps packages provide a command line utility that allows a user to convert a plain text file to a PostScript using Pango.

Bug Fix

BZ#618271

Prior to this update, the presence of certain non-printable characters in the input file could cause paps to get stuck in an infinite loop, consuming all available system memory. With this update, the underlying source code has been modified to prevent this behavior, and such memory leaks no longer occur.

Users of paps are advised to upgrade to these updated packages, which resolve this issue.

1.203. parted

1.203.1. RHBA-2011:0675 — parted bug fix and enhancement update

An updated parted package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The GNU Parted program allows you to create, destroy, resize, move, and copy hard disk partitions. Parted can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.

Bug Fixes

BZ#693852

Previously, when a user ran the parted program on the IBM System z platform, the character buffer for the fdasd_check_api_version() function was too short, causing a buffer overflow. This has been fixed by doubling the buffer. The buffer overflow does not occur anymore.

BZ#642476

Although the parted program's help information, accessed by running "parted --help", contained a usage example and a description for the "align-check" command, this information was missing from the corresponding manual page. This update corrects the parted(8) manual page to include a description of the "align-check" command.

Enhancement

BZ#618255

In order to help tools such as Anaconda support 4KB sector drives, the libparted-provided ped_device_get_optimum_alignment function now prefers to align partitions to 1MB whenever possible. This change has negligible effect on the parted command line tool.

All users of parted are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

1.204. perl

1.204.1. RHSA-2011:0558 — Moderate: perl security and bug fix update

Updated perl packages that fix three 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Perl is a high-level programming language commonly used for system administration utilities and web programming. The Perl CGI module provides resources for preparing and processing Common Gateway Interface (CGI) based HTTP requests and responses.

Security Fixes

CVE-2010-2761

It was found that the Perl CGI module used a hard-coded value for the MIME boundary string in multipart/x-mixed-replace content. A remote attacker could possibly use this flaw to conduct an HTTP response splitting attack via a specially-crafted HTTP request.

CVE-2010-4410

A CRLF injection flaw was found in the way the Perl CGI module processed a sequence of non-whitespace preceded by newline characters in the header. A remote attacker could use this flaw to conduct an HTTP response splitting attack via a specially-crafted sequence of characters provided to the CGI module.

CVE-2011-1487

It was found that certain Perl string manipulation functions (such as uc() and lc()) failed to preserve the taint bit. A remote attacker could use this flaw to bypass the Perl taint mode protection mechanism in scripts that use the affected functions to process tainted input.

These packages upgrade the CGI module to version 3.51. Refer to the CGI module's Changes file for a full list of changes.

Bug Fixes

BZ#626330

When using the "threads" module, an attempt to send a signal to a thread that did not have a signal handler specified caused the perl interpreter to terminate unexpectedly with a segmentation fault. With this update, the "threads" module has been updated to upstream version 1.82, which fixes this bug. As a result, sending a signal to a thread that does not have the signal handler specified no longer causes perl to crash.

BZ#640716

Prior to this update, the perl packages did not require the Digest::SHA module as a dependency. Consequent to this, when a user started the cpan command line interface and attempted to download a distribution from CPAN, they may have been presented with the following message:

```
    CPAN: checksum security checks disabled because Digest::SHA not
installed.
Please consider installing the Digest::SHA module.
```

This update corrects the spec file for the perl package to require the perl-Digest-SHA package as a dependency, and cpan no longer displays the above message.

BZ#640720

When using the "threads" module, continual creation and destruction of threads could cause the Perl program to consume an increasing amount of memory. With this update, the underlying source code has been corrected to free the allocated memory when a thread is destroyed, and the continual creation and destruction of threads in Perl programs no longer leads to memory leaks.

BZ#640729

Due to a packaging error, the perl packages did not include the "NDBM_File" module. This update corrects this error, and "NDBM_File" is now included as expected.

BZ#609492

Prior to this update, the prove(1) manual page and the "prove --help" command listed "--fork" as a valid command line option. However, version 3.17 of the Test::Harness distribution removed the support for the fork-based parallel testing, and the prove utility thus no longer supports this option. This update corrects both the manual page and the output of the "prove --help" command, so that "--fork" is no longer included in the list of available command line options.

Users of Perl, especially those of Perl threads, are advised to upgrade to these updated packages, which correct these issues.

1.204.2. RHSA-2011:1424 — Moderate: perl security update

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

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

Perl is a high-level programming language commonly used for system administration utilities and web programming.

Security Fixes

CVE-2011-2939

A heap-based buffer overflow flaw was found in the way Perl decoded Unicode strings. An attacker could create a malicious Unicode string that, when decoded by a Perl program, would cause the program to crash or, potentially, execute arbitrary code with the permissions of the user running the program.

CVE-2011-3597

It was found that the "new" constructor of the Digest module used its argument as part of the string expression passed to the eval() function. An attacker could possibly use this flaw to execute arbitrary Perl code with the privileges of a Perl program that uses untrusted input as an argument to the constructor.

All Perl users should upgrade to these updated packages, which contain backported patches to correct these issues. All running Perl programs must be restarted for this update to take effect.

1.205. perl-Mozilla-LDAP

1.205.1. RHBA-2011:0529 — perl-Mozilla-LDAP bug fix update

An updated perl-Mozilla-LDAP package that fixes several bugs and ensures that perl-Mozilla-LDAP always uses the OpenLDAP C SDK, is now available for Red Hat Enterprise Linux 6.

perl-Mozilla-LDAP is an LDAP Perl module that wraps the OpenLDAP client libraries.

Bug Fixes

BZ#644093

The perl-Mozilla-LDAP package has been upgraded to upstream version 1.5.3, which provides a number of bug fixes over the previous version.

BZ#610902

Previously, the Mozilla Perl LDAP SDK was a wrapper around the Mozilla C LDAP SDK (mozldap). Now that mozldap has been dropped from RHEL 6, in order to support legacy applications that still use the Mozilla Perl LDAP SDK, it has been ported to use OpenLDAP instead of mozldap. Applications that use the Mozilla Perl LDAP SDK should not notice any difference between the versions that use mozldap and the new one that uses OpenLDAP.

Users are advised to upgrade to this updated perl-Mozilla-LDAP package, which fixes these bugs.

1.206. perl-Sys-Virt

1.206.1. RHEA-2011:0767 — perl-Sys-Virt enhancement update

An updated perl-Sys-Virt package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The perl-Sys-Virt package provides an API for managing virtual machines from Perl, using the libvirt library.

Enhancement

BZ#675120

The Sys::Virt module has been updated to provide support for the new application programming interfaces (APIs) introduced between version 0.8.1 and 0.8.7 of the libvirt library.

All users of perl-Sys-Virt are advised to upgrade to this updated package, which adds this enhancement.

1.207. php

1.207.1. RHBA-2011:0615 — php bug fix and enhancement update

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

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server. It offers developers a built-in database integration and a solution to write dynamically generated web pages.

The php packages have been upgraded to upstream version 5.3.3, which provides a number of bug fixes and adds multiple enhancements over the previous version. It also introduces one backwards-incompatible language change in that only a function named "__construct" is now treated as a constructor in a namespaced class. This change has no effect on non-namespaced classes. (BZ#645591)

Bug Fix

BZ#655118

Previously, the check to prevent the "extract()" function overwriting the "$GLOBALS" variable was not working properly when using the default "EXTR_OVERWRITE" mode. The fix for this bug has been provided so that the check works as expected now.

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

1.208. php-pecl-memcache

1.208.1. RHEA-2011:0794 — php-pecl-memcache bug fix and enhancement update

An updated php-pecl-memcache package that fixes multiple bugs and adds one enhancement is now available for Red Hat Enterprise 6.

The php-pecl-memcache package enables PHP scripts to use the memcached caching daemon.

The php-pecl-memcache package has been rebased to version 3.0.5 which fixes multiple bugs and adds MemcachePool class support for the findServer() method. (BZ#638887)

Bug Fixes

BZ#638887

Previously, the "delete" methods failed for some memcached server versions due to a protocol error. With this update, the "delete" method works as expected.

BZ#638892

Previously, integer, float, and boolean values with enabled compression could not be retrieved successfully due to an issue with the compression flag. With this update, stored values are retrieved successfully.

BZ#672363

Previously, the memcache module aborted with a segmentation fault on the 64-bit PowerPC platform. This update resolves this problem and memcache runs on the 64-bit PowerPC architecture as expected.

BZ#604559

Previously, php-pecl-memcache contained extra characters after %{?dist}. This update deletes these characters.

All php-pecl-memcache users are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

1.209. php53

1.209.1. RHSA-2011:1423 — Moderate: php53 and php security update

Updated php53 and php packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 respectively.

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

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fixes

CVE-2011-2483

A signedness issue was found in the way the PHP crypt() function handled 8-bit characters in passwords when using Blowfish hashing. Up to three characters immediately preceding a non-ASCII character (one with the high bit set) had no effect on the hash result, thus shortening the effective password length. This made brute-force guessing more efficient as several different passwords were hashed to the same value.

CVE-2011-0708

Note: Due to the CVE-2011-2483 fix, after installing this update some users may not be able to log in to PHP applications that hash passwords with Blowfish using the PHP crypt() function. Refer to the upstream "CRYPT_BLOWFISH security fix details" document.

An insufficient input validation flaw, leading to a buffer over-read, was found in the PHP exif extension. A specially-crafted image file could cause the PHP interpreter to crash when a PHP script tries to extract Exchangeable image file format (Exif) metadata from the image file.

CVE-2011-1466

An integer overflow flaw was found in the PHP calendar extension. A remote attacker able to make a PHP script call SdnToJulian() with a large value could cause the PHP interpreter to crash.

CVE-2011-1468

Multiple memory leak flaws were found in the PHP OpenSSL extension. A remote attacker able to make a PHP script use openssl_encrypt() or openssl_decrypt() repeatedly could cause the PHP interpreter to use an excessive amount of memory.

CVE-2011-1148

A use-after-free flaw was found in the PHP substr_replace() function. If a PHP script used the same variable as multiple function arguments, a remote attacker could possibly use this to crash the PHP interpreter or, possibly, execute arbitrary code.

CVE-2011-1469

A bug in the PHP Streams component caused the PHP interpreter to crash if an FTP wrapper connection was made through an HTTP proxy. A remote attacker could possibly trigger this issue if a PHP script accepted an untrusted URL to connect to.

CVE-2011-1471

An integer signedness issue was found in the PHP zip extension. An attacker could use a specially-crafted ZIP archive to cause the PHP interpreter to use an excessive amount of CPU time until the script execution time limit is reached.

CVE-2011-1938

A stack-based buffer overflow flaw was found in the way the PHP socket extension handled long AF_UNIX socket addresses. An attacker able to make a PHP script connect to a long AF_UNIX socket address could use this flaw to crash the PHP interpreter.

CVE-2011-2202

An off-by-one flaw was found in PHP. If an attacker uploaded a file with a specially-crafted file name it could cause a PHP script to attempt to write a file to the root (/) directory. By default, PHP runs as the "apache" user, preventing it from writing to the root directory.

All php53 and php users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

1.210. pidgin

1.210.1. RHSA-2011:0616 — Low: pidgin security and bug fix update

Updated pidgin packages that fix multiple security issues and various bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. 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.

Security Fix

CVE-2011-1091

Multiple NULL pointer dereference flaws were found in the way the Pidgin Yahoo! Messenger Protocol plug-in handled malformed YMSG packets. A remote attacker could use these flaws to crash Pidgin via a specially-crafted notification message.

Red Hat would like to thank the Pidgin project for reporting these issues. Upstream acknowledges Marius Wachtler as the original reporter.

Bug Fixes

BZ#684685

Previous versions of the pidgin package did not properly clear certain data structures used in libpurple/cipher.c when attempting to free them. Partial information could potentially be extracted from the incorrectly cleared regions of the previously freed memory. With this update, data structures are properly cleared when freed.

BZ#616917

This erratum upgrades Pidgin to upstream version 2.7.9. For a list of all changes addressed in this upgrade, refer to http://developer.pidgin.im/wiki/ChangeLog

BZ#633860, BZ#640170

Some incomplete translations for the kn_IN and ta_IN locales have been corrected.

Users of pidgin should upgrade to these updated packages, which resolve these issues. Pidgin must be restarted for this update to take effect.

1.211. plymouth

1.211.1. RHBA-2011:0686 — plymouth bug fix update

Updated plymouth packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

Plymouth provides an attractive graphical boot animation in place of the text messages that are normally displayed. Text messages are instead redirected to a log file for viewing after boot.

Bug Fixes

BZ#625209

When two monitors shared one controller during a system boot, a blank screen appeared on both monitors. Consequently, users with this configuration experienced prolonged blank screens during boot-up and shutdown, and a choppy splash animation on any other external monitor. With this update, this bug has been fixed and the splash animation is now smooth and is displayed on all external monitors.

BZ#631924

Previously, the plymouth daemon terminated unexpectedly if there were any "console=" entries on the kernel command line. As a consequence, boot messages were not properly logged. With this update, this bug has been fixed, the plymouth daemon now handles console entries on the kernel command line without any crashes and boot messages are written to the log file as expected.

BZ#612665

Previously, the system prompted for a password on boot but provided no hint as to what the password was for. That caused unnecessary confusion for some users, who didn't know which of their passwords to enter. With this update, a hard drive icon has been added to prompts associated with encrypted disk volumes and the password prompts for encrypted disks are now easy to recognize.

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

1.212. portreserve

1.212.1. RHBA-2011:1285 — portreserve bug fix update

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

The portreserve package helps services with well-known ports that lie in the portmap range. It prevents portmap from occupying a real service's port by occupying it itself, until the real service tells it to release the port, generally in the init script.

Bug Fix

BZ#734765

Prior to this update, the portreserve daemon exited after the first port was released. As a result, all ports that services registered for portreserve were released when one of these services asked for its port to be released. With this update portreserve releases now only the requested ports.

All portreserve users are advised to upgrade to this update, which fixes this bug.

1.213. postfix

1.213.1. RHSA-2011:0843 — Moderate: postfix security update

Updated postfix 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.

Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), and TLS.

Security Fix

CVE-2011-1720

A heap-based buffer over-read flaw was found in the way Postfix performed SASL handlers management for SMTP sessions, when Cyrus SASL authentication was enabled. A remote attacker could use this flaw to cause the Postfix smtpd server to crash via a specially-crafted SASL authentication request. The smtpd process was automatically restarted by the postfix master process after the time configured with service_throttle_time elapsed.

Note: Cyrus SASL authentication for Postfix is not enabled by default.

Red Hat would like to thank the CERT/CC for reporting this issue. Upstream acknowledges Thomas Jarosch of Intra2net AG 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.

1.214. postgresql

1.214.1. RHSA-2011:1377 — 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).

Security Fix

CVE-2011-2483

A signedness issue was found in the way the crypt() function in the PostgreSQL pgcrypto module handled 8-bit characters in passwords when using Blowfish hashing. Up to three characters immediately preceding a non-ASCII character (one with the high bit set) had no effect on the hash result, thus shortening the effective password length. This made brute-force guessing more efficient as several different passwords were hashed to the same value.

Note: Due to the CVE-2011-2483 fix, after installing this update some users may not be able to log in to applications that store user passwords, hashed with Blowfish using the PostgreSQL crypt() function, in a back-end PostgreSQL database. Unsafe processing can be re-enabled for specific passwords (allowing affected users to log in) by changing their hash prefix to "$2x$".

For Red Hat Enterprise Linux 6, the updated postgresql packages upgrade PostgreSQL to version 8.4.9. Refer to the PostgreSQL Release Notes for a full list of changes.

For Red Hat Enterprise Linux 4 and 5, the updated postgresql packages contain a backported patch.

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.

1.214.2. RHBA-2011:0810 — postgresql bug fix update

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

PostgreSQL is an advanced object-relational database management system (DBMS) that supports most SQL constructs.

Bug Fix

BZ#694249

Previously, PL/pgSQL functions could have failed with an error if they used composite types as their arguments or result types. This happened if a column was dropped in the table underlying the composite type. This update adapts the source code that handles these situations so that such functions work correctly.

All users of postgresql are advised to upgrade to these updated packages, which resolve this bug.

1.215. powerpc-utils

1.215.1. RHBA-2011:0682 — powerpc-utils bug fix and enhancement update

An updated powerpc-utils package that fixes various bugs and adds an enhancement is now available.

The powerpc-utils package contains utilities for PowerPC platform.

Bug Fixes

BZ#659664

The man pages for several powerpc-utils executables (drmgr, lsdevinfo, lsprop, lsslot, nvsetenv, ppc64_cpu and rtas_event_decode) were not included in Red Hat Enterprise Linux 6.0. Man pages for these executables have now been added to powerpc-utils.

BZ#659696

The man page for "ofpathname" omitted several options and contained a typographical error. These issues have been corrected.

BZ#674421

Previously, the short version of the nvram "--verbose" flag, "-v", did not register as a valid flag. This option has been added to nvram and now works, consistent with its description in the man page.

BZ#679413

"ofpathname" uses /usr/bin/bc, but the powerpc-utils package does not depend on bc. ofpathname now checks whether bc is installed, and requests the user install it if this package is not found.

BZ#693802

The drmgr command incorrectly checked the "is_removable" field to determine the number of logical memory blocks available for a remove operation, even when AMS ballooning was active. Memory removal no longer relies on "is_removable" when ballooning is active.

Enhancement

BZ#632690

Support for partition hibernation has been added. This allows suspension for longer than 5-10 seconds, saving partition state to persistent storage, and freeing resources in use by that partition.

Users are advised to upgrade to this updated powerpc-utils package, which resolves these issues.

1.215.2. RHBA-2011:0819 — powerpc-utils bug fix update

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

The powerpc-utils package contains utilities for PowerPC platform.

Bug Fix

BZ#702566

Removing DLPAR (Dynamic Logical Partitioning) memory caused the kernel to panic due to improper handling of the memory off-lining procedure. This update corrects the code so that drmgr, the dynamic memory manager, now properly off-lines memory, with the result that removing DLPAR memory no longer causes a kernel crash.

All PowerPC users are advised to upgrade to this updated package, which resolves this issue.

1.216. powertop

1.216.1. RHBA-2011:0522 — powertop bug fix and enhancement update

An updated powertop package that fixes a bug and adds an enhancement is now available for Red Hat Enterprise Linux 6.

PowerTOP is a tool to detect all the software components that make a computer consume more than necessary power when idle.

Bug Fix

BZ#628514

Previously, PowerTOP could not run processes without a valid terminal. This update backports the TTY handling from powertop 1.13. Now, PowerTOP runs without a terminal in dump mode.

Enhancement

BZ#610464

Previously, PowerTOP could not detect whether hardware used the Intel Turbo Boost functionality. This update adds support for Intel Dynamic Acceleration (IDA) and Intel Turbo Boost.

All PowerTOP users are advised to upgrade to this updated package which fixes this bug and adds this enhancement.

1.217. prelink

1.217.1. RHBA-2011:0786 — prelink bug fix update

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

The prelink utility is used to modify ELF shared libraries and executables. This reduces the number of relocations that need to be resolved at runtime, and thus enables faster start-up.

Bug Fix

BZ#653635

When the prelink utility was used to modify executables or shared libraries, it did not preserve the corresponding access control lists (ACL) other than SELinux context. This update ensures that the ACLs are preserved as expected.

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

1.218. procps

1.218.1. RHBA-2011:0708 — procps bug fix update

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

The procps package contains a set of system utilities that provide system information. The procps package includes ps, free, skill, snice, sysctl, tload, top, uptime, vmstat, w, and watch.

Bug Fixes

BZ#596948

The vmstat disk device field was, previously, restricted to 15 characters. The Linux kernel allows for device names up to 32 characters, however, and the vmstat restriction resulted in two unwelcome behaviors. First, device names up to 31 characters were displayed correctly by "vmstat -d", although characters after the fifteenth were truncated. More significantly, devices with 32-character names were not displayed by "vmstat -d" at all. With this update, the vmstat disk device field now supports up to 32 characters, ensuring all devices are displayed properly in "vmstat -d" output.

BZ#622389

The sysctl command's man page described the "-A" switch as displaying "all values currently available in table form." This is incorrect: "-A" is equivalent to "-a", simply displaying all currently available values. This update includes an updated man page that corrects the error. As well, this updated man page includes a new NOTES entry, documenting the interaction between modules loaded after sysctl is run and sysctl itself.

BZ#684031

Previously applied procps patches contained three memory leaks, all of which can lead to procps utilities hanging. This update closes the leaks, ensuring the potential hangs do not, now, occur.

All procps users are advised to upgrade to this updated package, which resolves these issues.

1.219. psacct

1.219.1. RHBA-2012:0724 — psacct bug fix update

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

The psacct packages contain utilities for monitoring process activities, including ac, lastcomm, accton, dump-acct and sa. The "ac" command displays statistics about how long users have been logged on. The "lastcomm" command displays information about previously executed commands. The "accton" command turns process accounting on or off. The "dump-acct" command transforms the output file from the accton format to a human-readable format. The "sa" command summarizes information about previously executed commands.

Bug Fix

BZ#828725

Previously, improper data type detection could have caused an arithmetic overflow. As a consequence, the dump-acct tool reported incorrect elapsed time values. A patch has been applied so that correct values are reported with this update.

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

1.220. pykickstart

1.220.1. RHBA-2011:0662 — pykickstart bug fix and enhancement update

An updated pykickstart package that fixes several bugs and adds a number of enhancements is now available.

The pykickstart package is a python library used to manipulate kickstart files.

Bug Fixes

BZ#668050

The ksflatten tool included with pykickstart erroneously output any %include statements along with the content included by these statements. The original %include statements are now removed when the referenced content is included.

BZ

The documentation included in pykickstart was not referenced correctly, so no information was available to users. This has been corrected and useful documentation is now included. (No BZ#)

Enhancements

BZ#554870

The bootloader command now takes an additional "--iscrypted" option. Since GRUB supports multiple encryption mechanisms and can automatically detect which to use based on the encrypted password, this new option should be used whenever an encrypted password is provided. This takes the place of the previous "--md5pass=" option.

BZ#660340

The "url" and "repo" commands now take an additional "--noverifyssl" option. Use this option to prevent anaconda from checking the validity of the SSL certificate of your source when using HTTPS.

BZ#668417

Three new network options have been added to pykickstart: "--activate", "--nodefroute", and "--bootproto=ibft". These enable users to install to iSCSI target systems that use a network card other than the system's network configuration.

All users of pykickstart are advised to upgrade to this package, which fixes these bugs and adds these enhancements.

1.221. python

1.221.1. RHSA-2011:0554 — Moderate: python security and bug fix update

Updated python packages that fix three security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having 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.

Python is an interpreted, interactive, object-oriented programming language.

Security Fixes

CVE-2011-1521

A flaw was found in the Python urllib and urllib2 libraries where they would not differentiate between different target URLs when handling automatic redirects. This caused Python applications using these modules to follow any new URL that they understood, including the "file://" URL type. This could allow a remote server to force a local Python application to read a local file instead of the remote one, possibly exposing local files that were not meant to be exposed.

CVE-2010-3493

A race condition was found in the way the Python smtpd module handled new connections. A remote user could use this flaw to cause a Python script using the smtpd module to terminate.

CVE-2011-1015

An information disclosure flaw was found in the way the Python CGIHTTPServer module processed certain HTTP GET requests. A remote attacker could use a specially-crafted request to obtain the CGI script's source code.

This errata upgrades Python to version 2.6.6 (BZ#627301), and includes a number of bug fixes and enhancements.

Bug Fixes

BZ#603073

The **pydoc -k** command performs a keyword search of the synopses in all installed Python modules. This command failed on modules that did not import, resulting in a traceback. **pydoc -k** now ignores modules that have import exceptions, allowing searches on the remaining modules.

BZ#625393

A minor incompatibility with SELinux in one of the **commands** module selftests was corrected.

BZ#625395

The python-tests subpackage was missing some test files and directories used by the selftests for **lib2to3**. This update adds the missing content to the subpackage.

BZ#626756

Previously, the **in** operator for dbm mappings erroneously returned **False** for all keys on big-endian 64-bit builds of Python (64-bit PowerPC and IBM System z). This update fixes this issue.

BZ#634944

A harmless but unnecessary RPATH directive from the **_sqlite3.so** module was removed. Execution and "#!" lines from **.py** files within the standard library that did not require these lines were also removed.

BZ#637895

Previously, the **urllib2** module ignored the **no_proxy** variable for the FTP scheme. This could lead to programs such as **yum** erroneously accessing a proxy server for ftp:// URLs covered by a **no_proxy** exclusion. The **no_proxy** variable now overrides the **ftp_proxy** variable, enforcing this exclusion.

BZ#639222

Previously, the IDLE Python IDE used a hard-coded port (8833) when communicating between the shell and the execution sub-processes. Attempts to use more than one instance of IDLE on one computer failed with a "Port Binding Error" dialog box. This update backports a patch from Python 2.7 to use an ephemeral port instead, resolving this issue.

BZ#639392

On AMD64 and Intel 64 architectures, running **gdb** (configured using the **--with-python** option) on python applications to generate backtraces caused a traceback error. **python-gdb.py**, the python module that deals with the case of debugging a python process, was updated to prevent this.

BZ#649274

Using an invalid username or password while attempting to authenticate against HTTPS via the **urllib2** module resulted in infinite recursion. This behavior has been patched, and **urllib2**2 now attempts authentication a maximum of five times before authentication is considered failed.

BZ#650588

Previously, Python programs that used **ulimit -n** to enable communication with large numbers of subprocesses could still monitor only 1024 file descriptors at a time, due to the subprocess module using the **select** system call. This could cause an exception:

```
ValueError: filedescriptor out of range in select()
```

The module now uses the **poll** system call, removing this limitation.

BZ#669847

Basic HTTP authentication via the **urllib2** module was limited to six requests because the **retried** attribute was not reset when authentication was successful. This attribute is now reset, and authentication requests work as expected.

BZ#677392

The **test_structmembers** unit test failed on big-endian 64-bit builds of Python (64-bit PowerPC and IBM System z) because a variable was not well-defined. The variable is now defined correctly, and the unit test works as expected. Note that this issue was discovered and corrected during development, and was not encountered in production systems in the field.

BZ#684991

Upgrading Python removed a call to the **PyErr_Clear()** method, which exposed an assertion failure in RhythmBox that resulted in RhythmBox crashing. Python now compensates for the RhythmBox assertion failure.

BZ#690315

A race condition was discovered in python **Makefile.pre.in**. The **make** command interprets a make rule with two dependents as two copies of the rule. On machines with more than one core, this could lead to race conditions in which the compiler attempted to read a partially-overwritten file. This resulted in syntax or link errors when attempting to build python on machines with multiple cores. A check has been added to prevent this issue.

Enhancements

BZ#529274

This updated package now provides the python-ssl package, rendering the python-ssl package provided by the EPEL repository obsolete.

BZ#567229

The subprocess module now includes an optional **timeout** argument, which can be used by the **subprocess.call**, **Popen.communicate** and **Popen.wait** API entry points. This argument allows users to specify either an integer or a float value, which represents the number of seconds these processes will wait for a call to return before raising an exception of type **TimeoutExpired**.

BZ#569695

SystemTap static probes have been added to the Python runtime. Two example scripts are also provided: **`pyfuntop.stp`**, which provides a **`top`**-like view of all bytecode being executed; and **`systemtap-example.stp`**, which shows the function-call hierarchy of Python bytecode.

BZ#614680

Reference-handling bugs within C extension modules can lead to crashes when Python's garbage collector runs. The garbage collector now prints more informative messages to stderr when exiting due to unrecoverable reference errors.

All users of Python are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

1.222. python-dmidecode

1.222.1. RHBA-2011:1156 — python-dmidecode bug fix update

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

The python-dmidecode package provides a Python extension module that uses the code-base of the dmidecode utility and presents the data as Python data structures or as XML data using the libxml2 library.

Bug Fix

BZ#726614

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.

1.223. python-ethtool

1.223.1. RHBA-2011:0770 — python-ethtool bug fix and enhancement update

An updated python-ethtool package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The python-ethtool package provides Python bindings for the ethtool kernel interface. The python-ethtool utility allows users to query and change ethernet card settings.

Bug Fixes

BZ#605535

Previously, the manual pages for the command line tools pifconfig and pethtool were missing. This update adds the manual pages for both tools. Now, all tools are correctly documented in the python-ethtool package.

BZ#680269

Previously, the RETURN_STRING did not correctly handle the reference count of the Py_None singleton. Due to this problem, Python could abort with a fatal error if run repeatedly. This update corrects this error. Now, the reference for the Py_None singleton count is correctly handled and Python runs as expected.

Enhancement

BZ#605533

This update adds IPv6 support to python-ethtool.

All users of python-ethtool are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

1.224. python-meh

1.224.1. RHBA-2011:0760 — python-meh bug fix update

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

The python-meh package provides a python library for handling exceptions.

Bug Fixes

BZ#640929

Due to a conflicting shortcut used for both "Debug" and "Details" buttons, pressing the "Alt+D" key combination did not work. This update changes the keyboard shortcut for the "Debug" button to "Alt+G", resolving this issue.

BZ#670601

The "Url" field in the package's spec file has been corrected and no longer contains an invalid address.

All users of python-meh are advised to upgrade to this updated package, which resolves these issues.

1.225. python-nss

1.225.1. RHBA-2011:0607 — python-nss bug fix and enhancement update

An updated python-nss package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The python-nss package provides bindings for Network Security Services (NSS) that allow Python programs to use the NSS cryptographic libraries for SSL/TLS and PKI certificate management.

Bug Fix

BZ#619743

Previously, certain code sequences in the CPython modules caused the object reference count to be computed incorrectly which caused objects to be released too soon. Due to this behavior, a Python "memory error" exception was raised. This update adjusts the internal reference counting logic.

Enhancement

BZ#670951

This update adds several new classes, module functions, class methods, and properties.

All python-nss users are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

1.226. python-psycopg2

1.226.1. RHBA-2011:1091 — python-psycopg2 bug fix update

Updated python-psycopg2 packages that fix a bug are now available for Red Hat Enterprise Linux 6.

The python-psycopg2 packages provide the most popular PostgreSQL adapter for the Python programming language. At its core it fully implements the Python DB API 2.0 specifications. Several extensions allow access to many of the features offered by PostgreSQL.

Bug Fix

BZ#720306

Previously, if a second thread in a single application triggered the Python garbage collection while a copy operation was in progress, the copy operation terminated unexpectedly. With this update, appropriate object reference count adjustments have been added to the code, and this bug no longer occurs.

Users of python-psycopg2 are advised to upgrade to these updated packages, which fix this bug.

1.227. python-pycurl

1.227.1. RHBA-2011:0295 — python-pycurl bug fix update

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

PycURL is a Python interface to libcurl. PycURL is used to fetch objects identified by a URL from a Python program, similar to the urllib Python module.

Bug Fixes

BZ#565654

Prior to this update, calling the reset() method caused internal cURL properties to be lost, including the pointer to an error buffer. Consequent to this, when an error occurred, the resulting message could be empty. This update prevents this pointer from being lost, and error messages are now displayed as expected.

BZ#624559

When the reset() method was called, the number of references to the "Py_None" object was not counted properly. Consequent to this, Python could terminate unexpectedly with the following error message:

Fatal Python error: deallocating None Aborted (core dumped)

```
    With this update, the underlying source code has been modified to
address
this issue, and references to the "Py_None" object are now counted as
expected.
```

All users of python-pycurl are advised to upgrade to this updated package, which resolves these issues.

1.228. python-qpid

1.228.1. RHBA-2011:0801 — python-qpid bug fix update

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

The python-qpid package provides a python client library for the Apache Qpid implementation of the Advanced Message Queuing Protocol (AMQP).

The python-qpid package has been upgraded to upstream version 0.10, which provides numerous improvements over the previous version. (BZ#675825)

Users are advised to upgrade to this updated package, which resolves this issue.

1.229. python-rhsm

1.229.1. RHBA-2011:0818 — python-rhsm bug fix update

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

python-rhsm is a small library for communicating with the REST interface of a Red Hat Unified Entitlement Platform. This interface is used for the management of system entitlements, certificates, and access to content.

Bug Fix

BZ#702403

Previously, booting for the first time failed after a new Red Hat Enterprise Linux 6 installation was performed on HP DL360 Gen8. This was due to using invalid locale names, which caused a stack trace. The same problem also affected Red Hat Enterprise Linux 6's Subscription Manager. The problem has been fixed by using "C" as the default locale so that the Red Hat Enterprise Linux 6 first boot and Subscription Manager work as expected.

All users requiring python-rhsm should install this newly released package, which fixes this bug.

1.230. python-urlgrabber

1.230.1. RHBA-2011:0812 — python-urlgrabber bug fix update

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

The python-urlgrabber package provides urlgrabber, a high-level url-fetching package for the Python programming language and a corresponding utility of the same name. The urlgrabber package allows Python scripts to fetch data using the HTTP and FTP protocols, as well as from a local file system.

Bug Fix

BZ#695747

Due to changes to the curl packages that enabled the use of Network Security Services (NSS) by default, urlgrabber may have been unable to retrieve remote data. Consequent to this, an attempt to download repository data using the Yum package manager could fail with the "HTTP 403" status code. This update adapts urlgrabber to retain the compatibility with the curl packages, so that the applications that use this package (including Yum) can retrieve remote data as expected.

All users of python-urlgrabber are advised to upgrade to this updated package, which fixes this bug.

1.231. python-virtinst

1.231.1. RHBA-2011:0636 — python-virtinst bug fix and enhancement update

An updated python-virtinst package that fixes bugs and adds enhancements is now available for Red Hat Enterprise Linux 6.

The python-virtinst utility is a module that helps build and install libvirt based virtual machines.

The python-virtinst package has been upgraded to upstream version 0.500.5, which provides a number of bug fixes and enhancements over the previous version.

Bug Fixes

BZ#683100

When changing the acpi or apic values in virt-manager, virtinst would unset the values. This change now checks for the feature and ensures the value is retained allowing virtinst to parse domain features correctly.

BZ#683103

Added support for audio device 'ich6'.

BZ#683182

When specifying a wrong volume format type an error message would not display. This change informs the user by raising the appropriate error message when the storage pool cannot find the appropriate volume.

BZ#676995

The %d string format was being used in the --check-cpu error message causing an incorrect error message to display to the user. This fix uses the correct %s numeric format resulting in the correct error message to display.

BZ#678374

virt-install would fail to install the guest when the --nonsparse option was invoked. This issue has been resolved.

BZ#682697

When specifying spice as a graphic console for the guest and assigning a static port number the resulting output does not retain the port number. This fix ensures that the port number is retained.

BZ#658914

virt-install now includes support for unix sockets. This enhancement adds the ability to restrict the vnc connection to provide greater security to the guest.

BZ#678214

When converting the type of guest image from virt-image to vmx the resulting output is not a genuine status message. This fix changes the output into a useful format for the user.

BZ#683320

virt install would display the wrong error message when invoking --print-xml. This fix ensures the correct error message is displayed.

BZ#592172

virt-install now includes the --machine option. This is useful for manually choosing the guest machine type to emulate.

BZ#598157

An error message informing the user that libvirtd needs to be started is now displayed when virt-install is used without libvirtd running.

BZ#598170

virt-install would give the user an unclear error message and exit when given an invalid location to the installation tree. This forced the user to re-enter the installation command. This fix gives the user the appropriate error message and then prompts them for the valid location so the user does not have to re-enter the entire command.

BZ#607091

Unless the file image is already managed by libvirt, when a user specifies an existing file image with virt-install there is no warning displayed telling the user that the file will be overwritten. With this change the user is now prompted if the file already exists giving the user an opportunity to make any necessary corrections before overwriting the file image.

BZ#611205

qemu was not executing efficiently based on the storage type. With this fix, when async IO (aio), storage is block based (lvm, iscsi, fc) qemu is executed with aio=native. When the storage is file based (local filesystem, NFS), qemu is executed with aio=threads. This results in improved performance.

BZ#612842

virt-convert now includes support for qcow, qcow2, and cow formats.

BZ#616359

This change reports to the user the correct variant of Red Hat Enterprise Linux 3 Update 9 guest when it is detected as the previous version would report Red Hat Enterprise Linux 4.

BZ#616430

Previous versions of virt-install would prompt the user to insert installation media when the --prompt option was used and the install source was set to /dev/cdrom. This fix allows the installation to proceed if both of the preceeding conditions exist.

BZ#622661

Previous versions of virt-install would not display an error message if --extra-args is specified without --location. This fix displays an error message informing the user of the correct usage.

BZ#622684

virt-convert did not preserve the storage format in the generated xml configuration file causing some image files to fail to boot with the error "no bootable device". The xml configuration now correctly preserves the storage format allowing the image to boot successfully.

BZ#624714

Previous versions of virt-install checked the first bytes of the disk image's master boot to ensure the disk image was valid. However, this check only worked with raw disk. This update skips the check on non-raw disks.

BZ#638523

virt-install would put keymap into the generated xml file causing qemu internal keymaps to be used resulting in the possiblity of broken keyboards. This update fixes the default keymap for qemu and ensures correct operation of the -k option.

BZ#642719

virt-install may go into an indefinite loop when looking up a volume if the specified storage pool did not exist. This issue has been addressed and fixed.

BZ#672987

An error would occur and the installation would stop when instructing virt-install to build a virtual machine from a boot floppy by specifying device=floppy. This fix ensures that device=floppy is working appropriately.

Enhancements

BZ#658963

virt-install enhancements include the following options:

- --cpu for configuring CPU model/features
- --vcpus for specifying CPU topology
- --print-xml for generating guest XML
- --console for specifying virtio console device
- --channel for specifying guest communication channel
- --boot for setting post-install boot order, direct kernel/initrd boot, and enabling boot device menu.

All users of python-virtinst are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

1.231.2. RHBA-2011:1426 — python-virtinst bug fix update

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

The python-virtinst module helps build and install libvirt based virtual machines. It provides several command line utilities, such as virt-clone, which clones existing virtual machine images with the libvirt library.

Bug Fix

BZ#726615

The python-virtinst module often called the ifconfig program unnecessarily when parsing a domain XML file. If a domain contained many "direct" network interfaces, the virt-manager application responded so slowly that it could not be used properly. With this update, the redundant ifconfig calls have been removed from the code, and virt-manager now works well even with large number of "direct" network interfaces.

All users of python-virtinst are advised to upgrade to this updated package, which fixes this bug.

1.232. qemu-kvm

1.232.1. RHSA-2011:0534 — Important: qemu-kvm security, bug fix, and enhancement update

Updated qemu-kvm packages that fix two security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are linked to from the security descriptions below.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. qemu-kvm is the user-space component for running virtual machines using KVM.

Security Fixes

CVE-2011-1750

It was found that the virtio-blk driver in qemu-kvm did not properly validate read and write requests from guests. A privileged guest user could use this flaw crash the guest or, possibly, execute arbitrary code on the host.

CVE-2011-1751

It was found that the PIIX4 Power Management emulation layer in qemu-kvm did not properly check for hot plug eligibility during device removals. A privileged guest user could use this flaw crash the guest or, possibly, execute arbitrary code on the host.

Bug Fixes

BZ#482427

Previously, **qemu-kvm** did not have support for high resolution modes enabled, thus a user was unable to select a resolution higher than 1920x1080. This bug has been fixed by changing the value of the **VGA_RAM_SIZE** variable to 16 MB so that the user can now use high resolution modes.

BZ#498774

Previously, a virtual Windows guest user could have selected **`Safely Remove Hardware`** from the taskbar; however, hot-unplug functionality was not supported for various components, including the VGA device or virtual boot hard drive. This update disables hot-unplugging PCI devices from within Windows virtual guests.

IMPORTANT

Users should be cautious when choosing to hot-unplug any emulated device from within a virtual Windows guest.

BZ#515775

Previously, disk images which used the **VirtIO** framework could not be resized while **QEMU** was running. This update fixes the problem by adding the online disk resize functionality to **qemu-kvm**. The user is now able to resize the **VirtIO** online disks.

BZ#558256

Previously, several problems that were present in **QEMU**'s IDE CD-ROM emulation were causing the virtual guest's **Linux kernel** and **Anaconda** to fail while searching for an installation medium if the host system had multiple CPUs installed. This bug has been fixed by improving the IDE CD-ROM emulation.

NOTE

Under some circumstances, installation of a Red Hat Enterprise Linux 6 virtual guest can stall on searching for an installation medium; if this happens, just retry the search.

BZ#570467

Previously, the **`ksm`** and **`ksmtuned`** initscripts were not consistent in their behavior with other initscripts included in Red Hat Enterprise Linux 6. This update modifies the **`ksm`** and **`ksmtuned`** initscripts so that their behavior is now consistent.

BZ#581750

qemu-kvm terminated unexpectedly when an invalid argument was given to the ***`vhostfd`*** command line parameter due to improper handling of file descriptors. With this update, if an invalid argument is provided to the ***`vhostfd`*** parameter, **qemu-kvm** exits and displays an appropriate warning message.

BZ#585910

Previously, the handling of **Machine Check Exceptions (MCE)** in **qemu-kvm** did not properly handle **`BUS_MCEERR_AO SIGBUS`** signals and this caused **Software Recoverable Action Optional (SRAO) MCE** to kill the **qemu-kvm** process when a page was constantly used by the virtual guest. The problem has been fixed partly in this update, partly in the **kernel** update (see BZ#550938) so that **SRAO MCE** handling now works properly even if the page is being constantly read or written by the virtual guest.

BZ#588916

Under some circumstances, the **VirtIO** framework queue was filled if an application on a virtual guest repeatedly wrote to a **Virtio-Serial** character device while the host system was not processing the queue. Consequently, the guest entered an infinite loop and became unresponsive. Once the host

side of the character device was read from, the virtual guest returned to normal functionality. The erroneous behavior has been fixed in this update and no longer occurs.

BZ#596610

Previously, when a **Virtio-Serial** port or device was removed before a guest booted and initialized, the device caused **QEMU** to exit with an error message. This bug has been fixed in this update by not checking for any unused data on the host system if the state of the **VirtIO** framework on the virtual guest side is not yet initialized.

BZ#602205

Previously, the e1000 emulation in **qemu-kvm** did not support multi-buffer packets larger than the **`rxbuf_size`** option. This caused networking to stop if the maximum transmission unit (MTU) of the e1000 virtual network interface controller (NIC) was set to the value of 16110. With this update, support for larger multi-buffer packets has been added so that the MTU can now be set to 16110.

BZ#603413

The e1000 virtual network interface controller (NIC) did not support the "SECRC" field, with the result that triggering the network crash dump facility (**`netdump`**) on a Red Hat Enterprise Linux 3 virtual guest which was based on the i386 architecture caused a failure when using the e1000 NIC emulation. The support for the ***`SECRC`*** field has been added so that **`netdump`** now works correctly.

BZ#604992

The **qemu-kvm** documentation previously contained an empty function index in Chapter 7 of the **`qemu-doc.html`** file. The problem has been fixed by removing the empty index with this update.

BZ#608548

Previously, **QEMU** did not align memory properly for the ***`O_DIRECT`*** support. As a consequence, I/O requests to a device with large sector sizes (e.g. the CD-ROM drive) did not work in the **`cache=none`** mode. This update has fixed **QEMU** so that it uses a properly aligned memory for the I/O requests and I/O requests to devices like the CD-ROM drives now work as expected.

BZ#609016

Due to an 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 and **`ksmtuned`** now works as expected.

BZ#616187

Previously, the **qemu-kvm** options to enable VMware device emulation were exposed to a user, although the VMware device emulation functionality was not available in Red Hat Enterprise Linux 6. This has been fixed so that the emulation options are not exposed anymore.

BZ#616659

Previously, the migration of a virtual guest from a source with a user space back end to a destination with the **`vhost_net`** back end did not work. This has been fixed by adding support for a buffer, which can be merged, to the **`vhost_net`** back end so that the migration works as expected.

BZ#617119

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 with this update, and **kvm-qemu** now works as expected.

BZ#619168

In the case of certain memory allocation failures, **QEMU** terminated with only a self inflicted ***SIGABORT*** signal rather than clearly indicating the cause for failure to the user. This problem has been resolved so that an error message is now displayed, clearly indicating the failure cause.

BZ#619259

Previously, when **QEMU** was launched with the **`-cpu check`** command line option, the output was not as expected if a valid CPU model name was not provided. As a consequence, the **`-cpu check`** and **`-cpu enforce`** options did not work with the default CPU model and **QEMU** failed with a command line interface parsing error. The problem has been fixed so that it is now possible to enter "default" as a CPU model name, which allows the **`-cpu check`** and **`-cpu enforce`** options to function as expected.

BZ#621484

Previously, processes that ran within a virtual guest did not receive some of the **Virtio-Serial** data from processes that ran outside the virtual environment after the virtual guest's side closed a connection. This was due to **QEMU**'s character device interface failing to detect the other end of a socket that was closed until a read attempt timed out. This bug has been fixed with this update so that no **Virtio-Serial** data is now lost while silently being reported as written.

BZ#623552

Under certain circumstances, some pages, which were in the "dirty" state, were not transferred to the destination host and the **`scp`** command failed during a virtual machine migration in **qemu-kvm**. This bug has been fixed so that **`scp`** does not fail anymore during the migration.

BZ#623735

Previously, when a **VirtIO** network interface controller (NIC) was hot-plugged while **`vhost`** was set as a back end, **qemu-kvm** terminated unexpectedly. The fix for this problem has been provided with this update so that the **VirtIO** NIC hot plug works correctly.

BZ#624396

Previously, when a user hot-unplugged a **Virtio-Serial** device and then attempted to migrate a virtual machine, the migration failed. This was due to not removing the device's state from migration data from the source virtual machine. The source virtual machine then sent the device data to the destination virtual machine, which did not expect that device, resulting in migration failure. This bug has been fixed so that the migration now works as expected.

BZ#624607

When starting a virtual machine that uses thin-provisioning (COW) disk, **QEMU** could have failed to connect to the virtual I/O disk and the virtual machine would go into the pause state without returning much error information. **QEMU** now returns more verbose error information to help you debug any I/O-related errors.

BZ#624721

Previously, when a user provided **QEMU** an invalid (or non-existent) **`initrd`** file, **QEMU** failed. As a consequence, a virtual machine was not able to start, and **QEMU** did not display any error message to the user either. The fix for this bug has been provided by checking for the **`initrd`** file's validity and displaying an error message in case of the file's invalidity.

BZ#624767

Previously, the Paravirtualized Network Adapter (**virtio-net**) used a packet transmission algorithm that was using a timer to delay a transmission in an attempt to batch multiple packets together. This problem caused a higher **virtio-net** transmission latency. With this update, the default algorithm has been changed so that the **virtio-net** transmission latency is now significantly lower.

BZ#625319

Previously, there was a bug in the **removable** check for virtual media change for devices with the **if=none** option set. The bug caused a failure when a user changed the media of virtual floppy devices. This problem has been resolved with this update so that changing the media of virtual floppy devices now works without problems.

BZ#625333

Previously, the **-nodefconfig** option did not work correctly in that **QEMU** did not read an alternate **cpu-x86_64.conf** file and used the default **cpu-x86_64.conf** file instead when combined with the **-readconfig** option. This bug has been fixed so that the **-nodefconfig** option now works as intended and expected.

BZ#628634

Previously, **qemu-kvm** became unresponsive when it failed to start the**vhost_net** back end. The bug has been fixed in this update so that **qemu-kvm** now works as expected when the **vhost_net** back end is unable to start.

BZ#632257

Previously, feature flags defined for AMD CPU models were also erroneously used for Intel CPU models by **qemu64**. This problem has been resolved by removing the feature flags defined for AMD CPU models from the corresponding Intel CPU model definitions.

BZ#633699

Attempting to hot-plug a network interface controller (NIC) on a virtual machine with four or more gigabytes of assigned virtual memory failed with the following error message:

```
Device '[device_name]' could not be initialized
```

This update has fixed this bug so that hot-plugging a NIC in a virtual machine with four or more gigabytes of the virtual memory no longer fails.

BZ#634661

Under certain circumstances, when a user ran a Windows Server 2008 virtual machine with a **VirtIO** framework network interface controller (NIC), hot-unplugging the NIC caused **qemu-kvm** to terminate unexpectedly with a segmentation fault. This bug has been addressed with this update so that hot-unplugging such NIC while the virtual machine is active no longer causes **qemu-kvm** to fail.

BZ#635354

Previously, when a user reopened the block device backing file using the **qemu-img commit** command, the file was reopened with the wrong format (the format of the snapshot image), and the following error message was printed:

```
qemu-img: Error while committing image
```

This bug has been fixed so that the file is now reopened with the correct backing file format.

BZ#635418

Previously, the Kernel-based Virtual Machine (KVM) registered unconditionally so that the Kernel Samepage Merging (KSM) could only be enabled/disabled globally and not selectively for each virtual machine. This update introduces a new feature to **qemu-kvm** to selectively decide if KVM should register in KSM or not at virtual machine startup time. This allows a user to select higher performance virtual machines that will not risk being slowed down in memory de-duplication.

BZ#635527

Previously, there was no metadata caching performed for the Kernel-based Virtual Machine (KVM) Qcow2 disk image file format, resulting in poor performance of the **`qemu-img rebase`** command. In this update, a metadata cache for Qcow2 has been introduced, and thus performance is now improved.

BZ#635954

Previously, a user could attempt to migrate a virtual machine (VM) even if the VM was tied to hardware on the hosted system due to the device assignment. The fix for this bug has been provided in this update so that virtual machines with assigned devices will not allow a migration, ensuring the integrity of the VM. Migration is enabled again if all assigned devices are removed from the VM.

BZ#636494

Previously, when a user executed the **`qemu -cpu check`** and/or **`qemu -cpu enforce`** command, the CPU feature flags **`vmx`** and **`svm`** were not validated correctly. This could possibly cause a virtual guest's confusion if the feature flags were unintentionally exposed. This problem has been fixed by disallowing the **`vmx`** flag in all cases and the **`svm`** flag only if a nested Kernel-based Virtual Machine (KVM) is in effect.

BZ#637701

Previously, **QEMU** was unable to make live snapshots of an in-use disk image. This problem has been resolved so that a user is now able to make live snapshots by issuing the **`snapshot_blkdev`** command in the **QEMU monitor**.

BZ#638468

Previously, the VGA Bios (**`vgabios`**) for the QEMU Standard VGA expected to find the framebuffer memory at the magic address 0xe0000000. Due to the overlapping memory reservations, **qemu-kvm** aborted unexpectedly when the guest operating system tried to use the address space at 0xe0000000 for other spaces, e.g. mapping resources of hot-plugged PCI devices. This update changes **`vgabios`** to lookup the framebuffer memory in PCI space instead. Now, the address space at 0xe0000000 can freely be used by the guest operating system.

BZ#639437

Due to an error in the Russian keyboard layout, pressing the "**`/`**" and "**`|`**" keys with the Russian "ru" layout enabled produced the 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#641127

Under certain circumstances, e.g. when using an NFS file system, errors emitted by the **QEMU disk image utility** (**qemu-img**) were ignored when a user created a disk image using the **`qemu-img create`** command. In this update, error handling of the output of the **`qemu-img create`** command

has been made more reliable and the emitted errors are no longer ignored.

BZ#641833

Previously, there were several problems with the smart card support in **qemu-kvm**. These included waiting on the Name Service Switch (NSS) timeout during the startup of the smart card device. Also, the PC/SC Smart Card Daemon (**pcscd**) terminated unexpectedly when a user removed the card during a transaction. The last problem was that the device was only tested in a single card and reader setup so it only supported this particular reader/device setup. All these problems have been resolved in this update so that they no longer occur.

BZ#647308

Previously, Intel processors based on the Intel Xeon Processor E56XX, L56XX W36XX and X56XX families, and the Intel Xeon Processor E7 family were not defined as supported CPU models. As a consequence, support for the AES CPU feature flag and local attributes was missing for these Intel processors. The problem has been resolved so that these Intel processors are now included in the group of supported CPU models.

BZ#625948

Adding an rtl8139 network interface controller (NIC) to an active Windows 2008 guest could have resulted in the **qemu-kvm** process exiting. To work around this issue, shut down the virtual guest before adding additional rtl8139 NICs. Alternatively, install the virtio-net drivers and add a **VirtIO** NIC.

BZ#653536

The qemu-kvm package has been has been updated to improve the performance of converting a disk image by using the "qemu-img convert" command.

BZ#653591

If you attach a virtual I/O network interface card (NIC) that uses the rtl8139 driver to a live virtual host (commonly known as hotplugging), the virtual machine might not be able to migrate successfully because of an error in the rtl8139 driver. The driver has been updated so you can migrate virtual machines regardless of whether or not they have had a virtual I/O NIC attached to a live virtual host of not.

BZ#654682

The qemu-kvm package has been enhanced to add the 'drive_del' monitor command so that the libvirt package can force a disconnection between the guest and the host block device.

BZ#656198

A maximum of 16 ports were seen in the guest, even when you were using a serial virtual I/O device with more than 16 ports, so the guest was unable to communicate with any hosts on the ports beyond the 16th one. The guest was missing port instantiation messages because the queue size for outstanding requests from the host to the guest was too small. The queue size has now been increased to 32, enabling more outstanding requests at the same time, so now all of the allowed 31 ports can be instantiated at once.

BZ#658288

The qemu-kvm package now includes the -fake-machine patch, which adds a build-time option to enable -fake-machine. The -fake-machine option is disabled by default.

BZ#665025

When the network connection from the virtualization host to the VNC client was slow, the guest would miss clicks and movements of a virtual USB pointing device, so operations on the graphical user interfaces, including dragging and double-clicking, were difficult to perform. Now, virtual USB pointing devices buffer your clicks and movements so they behave as expected.

BZ#665299

The qemu-kvm package has been enhanced to automatically load and use the vhost-net kernel module, so performance is improved.

BZ#667188

If you detached a device to a live virtual host (commonly known as hotplugging), the qemu-kvm package did not release the memory that was used for storing device PCI Option ROM contents. Attaching and detaching devices with Option ROM caused the QEMU process size to grow. The management of memory that is used for PCI Option ROM of assigned devices has been updated so that when you remove a device, all resources that are consumed by that device are also removed.

BZ#670787

Devices consumed resources from a fixed resource pool as they were assigned to a virtual machine, and when the resource pool was exhausted, the virtual machine would unexpectedly shut down. The number of devices that can be assigned to a virtual machine has been limited to eight to avoid running out of resources, so adding devices to a virtual machine no longer triggers an unexpected shutdown.

BZ#671100

The format of some migration data was handled incorrectly, which in rare cases caused migration to fail. The format is now handled correctly and you can migrate successfully.

BZ#672191

The qemu-kvm package did not include flow control on the spice agent channel, so copying and pasting large amounts of text would make the package hang. Flow control has been added and you can now copy and paste of large amounts of text.

BZ#672229

If you detached a device to a live virtual host (commonly known as hotplugging), the qemu-kvm package did not release the memory that was used for storing device PCI Option ROM contents. Attaching and detaching devices with Option ROM caused the QEMU process size to grow. The management of memory that is used for PCI Option ROM of assigned devices has been updated so that when you remove a device, all resources that are consumed by that device are also removed.

BZ#672720

The buffer for USB control requests was too small for some devices (such as some USB cameras) when using USB passthrough, so these devices would make the qemu-kvm package display an error similar to the following: "'husb: ctrl buffer too small (3273 > 2048)'". The buffer for USB control requests has been increased from 2048 bytes to 8192 bytes, so USB passthrough now works for these devices.

BZ#674539

qemu-kvm tap code default for 'sndbuf' could prevent another guest from transmitting any packets. As a result, all networking could be blocked when sending packets to a guest which does not consume the packets. This is fixed by changing the default of the 'sndbuf' option to 0, which disables sndbuf. Now, guest networking is not blocked even when the recipient is not consuming the packets.

BZ#674562

Previously, guests running Red Hat Enterprise Linux 5 and older did not support Messaged Signaled Interrupts (MSI). On these guests, using vhost-net required higher CPU resources than userspace virtio. This update disables vhost-net for non-MSI guests, so non-MSI guests use userspace virtio-net instead of vhost-net, and get better performance.

BZ#675229

Installation of cpu-x86_64.conf into the host did not have the SRC_PATH prefix. As a result, out of tree builds failed to find the source configuration file and could not build. This update adds the missing SRC_PATH prefix to makefile, therefore building occurrs as expected.

BZ#676015

Previously, qemu-kvm enabled vhost when qemu NIC link was set to 'off'. Therefore, 'set_link <tap> off' did not work when using vhost-net. With this update, vhost is disabled when the 'set_link <tap> off' monitor command is used. The 'set_link <tap> off' monitor command now works when using vhost.

BZ#676529

Previously, creating a live snapshot for a non-existing disk triggered core dump. Now, attempting to save a snapshot for a non-existing disk yields an error message and returns qemu-kvm to the original image.

BZ#677712

A patch disabling the VMWare device emulation function caused migration from old to new qemu-kvm to fail. This issue has now been fixed, and updating qemu-kvm works as expected. Note that this bug was introduced and corrected during development, and was never seen on a production system in the field.

BZ#678208

Due to a bug in the locking logic of the spice code, qemu-kvm hanged when using certain versions of the qxl driver in the guest. This update fixes the locking logic in the spice code, so qemu-kvm does not hang anymore when using drivers such as xorg-x11-drv-qxl-0.0.12-5 in the guest.

BZ#678338

Descriptor status handling for e1000 emulation did not behave as expected, therefore using e1000 caused netperf or other workloads to fail when receiving large packets. This update fixes the e1000 emulation code according to the hardware specification with regards to the status byte on buffer descriptors. As a result, e1000 emulation now works under higher network load.

BZ#678524

Previously, all child processes were "reaped" without distinction by qemu-kvm's SIGCHLD handler. This SIGCHLD handler conflicted with the VM save code, therefore virtual machines could not be saved. This update allows the SIGCHLD handler to only reap specific child processes. qemu-kvm SIGCHLD handler no longer reaps processes created from VM save operations, so saving virtual machines succeeds.

BZ#680058

When devices were removed from QEMU, the device assignment code only removed resources that had been mapped into the guest address space. If an assigned device is removed before the guest mapped the device resources, open file handles could be leaked. Upon repetition, the QEMU process would reach its limit of open file handles. This update closes all file handles for assigned devices when the device is removed, so file handles are no longer leaked.

BZ#681777

During migration, the media_changed flag was not saved and restored in the floppy migration code, therefore floppy drives became unusable. The floppy migration code is now fixed, so transferring files to floppy drives works as expected.

BZ#682243

Due to a bug in the virtio-pci loading of the bus-master flag during migration, using PCI hotplug after live migration of a virtual machine disabled the virtio-net interface. This update fixes the bus master flag loading on virtio-pci migration code, so virtio-net works as expected with PCI hotplug after live migration.

BZ#683295

A bug in the QEMU option parse code caused the vhost_force option to be unusable. This issue has now been fixed, and vhost_force option can be used to force start vhost_net backend.

BZ#683877

Changing virtual CD-ROM images on a guest did not invalidate the previous disc's geometry information, so the new CD-ROM's disk size was not updated. With this update, guests properly detect changed discs and invoke their disc revalidation code, causing the correct disc geometry to be reported and used.

BZ#684076

An address conversion bug in the vhost migration dirty page handling code resulted in a segmentation error during live migration of KVM virtual machines. This update corrects the address conversion in the vhost migration dirty page handling code, so qemu-kvm no longer crashes during live migration.

BZ#685147

Devices that are attached to a virtual machine might continue direct memory access (DMA) operations after the virtual machine has been reset, which might result in DMA operations overwriting guest memory. Any devices that are attached to a virtual machine are now reset when the virtual machine is reset, so the devices are quiesced and no longer continue DMA operations after the virtual machine has been reset.

BZ#688058

A bug in the serial number setting code of the qemu-kvm package caused drive serial numbers to get truncated to eight characters. The code has been updated and the drive serial numbers are no longer truncated.

BZ#688119

qcow2_open() error handling returned a value of -1 rather than correct error codes, which led to misleading error messages because a value of -1 is interpreted as EPERM by callers. Also, qcow2 images with a version number of greater than two should return -ENOTSUP, but were instead detected as raw images. Correct -errno error return values have been added to the qcow2_open() function, so any permission errors and unsupported qcow versions are correctly reported when opening qcow2 images.

BZ#688146

qcow2 would incorrectly handle or ignore some errors, which could cause image corruption. Error handling fixes on qcow2 code have been backported, so qcow2 now handles errors more safely and avoids image corruption when errors occur.

BZ#688147

For a QCOW2 image that is larger than its base image, when handling a read request that extends over the end of the base image, the QCOW2 driver attempts to read beyond the end of the base image. However, these I/O requests would fail because of an error in the QCOW2 code. The code has been updated and now for a QCOW2 image that is larger than its base image, when handling a read request that extends over the end of the base image, I/O requests succeed.

BZ#688572

The spice-server would not switch back to server mouse mode if the guest spice-agent died, so users were left with a non-functional mouse. Now, the virtio-console notifies spice-chardev when a guest opens or closes, so the mouse is functional even when spice-agent is stopped in the guest.

BZ#690174

When virtio-serial loaded live migration data, it would not validate the port ID, which could crash qemu-kvm. The port ID is now validated, and virtio_serial_load() aborts incoming migration if it finds an invalid port ID.

BZ#690267

The performance of qemu_get_ram_ptr() was suboptimal and led to a higher use of CPU when booting a virtual machine. qemu_get_ram_ptr() has been updated and now skips some qlist manipulations if the ramblock that is found is already the first in the list, so virtual machine boot times have been improved.

BZ#691704

VGA memory region update notifications caused vhost-net to make many map flushing operations, which would slow booting of Windows guests with large amounts of memory (for example, 256GB). The virtual host now skips VGA memory regions when handling memory region update notifications, so the virtual host no longer slows booting of Windows guests with large amounts of memory.

BZ#693741

Because qemu-img tried to open backing files as read-write, the qemu-img rebase command failed if the new backing file was read-only. The qemu-img rebase command has been updated and can now open new backing files as read-only.

Enhancements

BZ#633394

This update increases the performance and scalability of the **VirtIO** framework by reducing the amount of time taken from virtual guests, and allowing the virtual guests CPU and I/O operations to run in parallel.

BZ#647307

This update adds support for KVM devices that make use of the MMIO PCI Base Address Registers (BARs), which are smaller than 4k (i.e. sub-4k MMIO PCI BARs).

BZ#632722

This update introduces support for tracing of events within **QEMU**; the tracing is similar in its style to **DTrace**. When used in conjunction with SystemTap, it is now possible to trace internal **QEMU** events such as I/O operations and memory allocations.

BZ#624790

This updates comes with an improved Kernel-based Virtual Machine (KVM) device assignment in that the PCI configuration space support has been improved to work with a broader assortment of devices, including the Exar X3100 series 10 Gigabit Ethernet cards.

BZ#645342

In this update, the ability to expose an emulated Intel HDA sound card to all virtual guests has been added. This update enables native sound support for many virtual guests, including the 64-bit version of Windows 7.

BZ#631832

The **`qemu-kvm`** man page has been updated with information on available **`-spice`** options.

All users of qemu-kvm should upgrade to these updated packages, which contain backported patches to resolve these issues, and [something about bug fixes in technical notes]. 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.

1.232.2. RHSA-2011:0919 — Important: qemu-kvm security and bug fix update

Updated qemu-kvm 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.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. qemu-kvm is the user-space component for running virtual machines using KVM.

Security Fixes

CVE-2011-2212

It was found that the virtio subsystem in qemu-kvm did not properly validate virtqueue in and out requests from the guest. A privileged guest user could use this flaw to trigger a buffer overflow, allowing them to crash the guest (denial of service) or, possibly, escalate their privileges on the host.

CVE-2011-2512

It was found that the virtio_queue_notify() function in qemu-kvm did not perform sufficient input validation on the value later used as an index into the array of virtqueues. An unprivileged guest user could use this flaw to crash the guest (denial of service) or, possibly, escalate their privileges on the host.

Red Hat would like to thank Nelson Elhage for reporting CVE-2011-2212.

Bug Fix

BZ#701771

A bug was found in the way vhost (in qemu-kvm) set up mappings with the host kernel's vhost module. This could result in the host kernel's vhost module not having a complete view of a guest system's memory, if that guest had more than 4 GB of memory. Consequently, hot plugging a vhost-

net network device and restarting the guest may have resulted in that device no longer working.

All users of qemu-kvm should upgrade to these updated packages, which contain backported patches to resolve these issues. 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.

1.232.3. RHBA-2011:1211 — qemu-kvm bug fix update

Updated qemu-kvm packages that resolve several issues are now available for Red Hat Enterprise Linux 6.

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on AMD64 and Intel 64 systems that is built into the standard Red Hat Enterprise Linux kernel. The qemu-kvm packages form the user-space component for running virtual machines using KVM.

Bug Fixes

BZ#726609

When the virsh dump command was executed with the "--live" option, the subsequent virsh dump command for the same domain led to undefined behavior. This was caused by a function trying to deallocate memory that had already been freed. To avoid this issue, the log field of the vhost device structure is now set to NULL after it has been passed to a deallocating routine. Running the virsh dump command repeatedly no longer leads to undefined behavior, and a core dump of a guest is now collected.

BZ#727468

Previously, a particular device using the tg3 driver failed to be re-assigned on a running KVM guest. The Broadcom Corporation NetXtreme BCM5761 Gigabit Ethernet PCIe network controller provides a PCI-Express Cap structure that is 8 bytes shorter than it should be according the PCI-Express 2.0 specification. This fact resulted in memory corruption when it was allocated for device assignment. The code has been modified to accept the reduced size of the structure. BCM5761 can now be successfully re-assigned.

BZ#727896

When KVM guests were launched with the "-device isa-serial" option instead of the "-serial" option, serial devices created were not visible by Windows guests. This issue arose because QEMU did not expose these devices in the guests' ACPI tables. With this fix, the guest's ACPI Differentiated System Description Table (DSDT) now properly senses the presence of serial devices and Windows guests can now see them properly.

All users of qemu-kvm are advised to upgrade to these updated packages, which resolve these issues.

1.232.4. RHEA-2011:1108 — qemu-kvm enhancement update

Enhanced qemu-kvm packages are now available for Red Hat Enterprise Linux 6.

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on AMD64 and Intel 64 systems that is built into the standard Red Hat Enterprise Linux kernel. The qemu-kvm packages form the user-space component for running virtual machines using KVM.

Enhancement

BZ#725543

Prior to this updated, a support statement in the text issued by the "qemu-kvm --help" command contained the following lines:

```
        WARNING: Direct use of qemu-kvm from the command line is
unsupported.
    WARNING: Only use via libvirt.
    WARNING: Some options listed here may not be available in future
releases.
```

With this update, this support statement has been modified to be more accurate, and it no longer claims that direct use of this command from the command line is unsupported: using qemu-kvm from the command line is just not recommended. Instead, Red Hat recommends using the libvirt tool as the stable management interface.

Users of qemu-kvm may want to upgrade to these updated packages, which add this enhancement.

1.232.5. RHBA-2011:1086 — qemu-kvm enhancement update

Updated qemu-kvm packages that add an enhancement 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 that is built into the standard Red Hat Enterprise Linux kernel. The qemu-kvm packages form the user-space component for running virtual machines using KVM.

Enhancement

BZ#720999

Due to Linux NFS client issues, the NFS request for the direct vectored I/O operation resulted in splitting a single I/O request into multiple requests, which had a serious impact on performance. The QEMU utility has been modified to detect files that exist in NFS when a request for vectored I/O operation comes to the server, and to use the QEMU_AIO_MISALIGNED flag to force such requests to be handled with a linear buffer.

All users of qemu-kvm should upgrade to these updated packages, which add this enhancement. In order for this update to take an effect, all running virtual machines have to be shut down and started again after this update is installed.

1.233. ql2400-firmware

1.233.1. RHBA-2011:0591 — ql2400-firmware bug fix and enhancement update

An updated ql2400-firmware package that provides several bug fixes and enhancements is now available for Red Hat Enterprise Linux 6.

The ql2400-firmware provides the firmware required to run the QLogic 2400 Series of mass storage adapters.

This update upgrades the ql2400 firmware to upstream version 5.03.16, which provides a number of bug fixes and enhancements over the previous version. (BZ#682847)

All users of QLogic 2400 Series Fibre Channel adapters are advised to upgrade to this updated package.

1.234. ql2500-firmware

1.234.1. RHBA-2011:0592 — ql2500-firmware bug fix update

An updated ql2500-firmware package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The ql2500-firmware package provides the firmware required to run the QLogic 2500 Series of mass storage adapters.

This update upgrades the ql2500 firmware to upstream version 5.03.16, which provides a number of bug fixes and enhancements over the previous version. (BZ#682848)

All users of QLogic 2500 Series Fibre Channel adapters are advised to upgrade to this updated package.

1.235. qpid-cpp

1.235.1. RHBA-2011:0771 — qpid-cpp bug fix and enhancement update

Updated qpid-cpp packages that fix several bugs and add various enhancements are now available.

The qpid-cpp packages provide a message broker daemon that receives, stores and routes messages using the open AMQP messaging protocol along with run-time libraries for AMQP client applications developed using Qpid C++. Clients exchange messages with an AMQP message broker using the AMQP protocol

The qpid-cpp package has been upgraded to upstream version 0.10, which provides numerous improvements over the previous version. (BZ#675821, BZ#631002)

Bug Fixes

BZ#615000

Prior to this update, qpid-cpp man pages were generated using the help2man package. However, if the package was not installed on the system, the man pages were built incorrectly. With this update, man pages are now correctly generated without the help2man package.

BZ#617260

A qmf agent caused a running broker to crash when the message queue limits were exceeded. This was due to the corruption of various lists/maps in the broker's management agent. This update modifies all the corrupted lists/maps and a qmf agent no longer crashes a broker.

Enhancements

BZ#659098

The QMFv2 C++ library and the QMFv2 Ruby binding have been added to the qpid-cpp component.

BZ#662826

QMFv1 now supports multiple brokers for a QMF namespace.

Users are advised to upgrade to these updated qpid-cpp packages, which resolve these issues and add these enhancements.

1.235.2. RHBA-2011:1398 — qpid-cpp bug fix update

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

The qpid-cpp packages provide a message broker daemon that receives, stores and routes messages using the open AMQP messaging protocol along with run-time libraries for AMQP client applications developed using Qpid C++. Clients exchange messages with an AMQP message broker using the AMQP protocol.

Bug Fixes

BZ#728586

Due to a regression, a memory leak was introduced that prevented the broker from correctly releasing messages. Consequently, the broker's memory footprint grew indefinitely. A patch has been provided to address this issue, and the memory leak no longer occurs in the described scenario.

BZ#734608

After the upgrade of MRG Messaging from version 1.2 to version 1.3, the qpidd daemon terminated unexpectedly on some of the cluster nodes. With this update, the broker code has been fixed to handle all cases when a faulty client sends frames before completely opening the connection, thus fixing this bug.

BZ#732063

Previously, specifying an invalid IP address for a destination broker caused a repeatable file descriptor leak. A patch has been provided to address this issue, and the file descriptor leak no longer occurs in the described scenario.

BZ#733543

Prior to this update, when a large message (over 4KB) was sent from the python-qpid client to the broker, the connection became unresponsive and other clients were unable to connect to the broker. This bug has been fixed, and clients no longer hang in the described scenario.

BZ#690107

Under heavy load, the broker generated a large number of timer late/overrun warning messages. Though the messages themselves were usually inoffensive, the time to log them individually caused long (up to several seconds) delays and inflated log files. With this update, logging output for these messages has been restricted to the "--log-enabled=info" option, thus preventing this bug.

All users of qpid-cpp are advised to upgrade to these updated packages, which fix these bugs.

1.236. qpid-tests

1.236.1. RHBA-2011:0802 — qpid-tests bug fix update

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

The qpid-tests package contains conformance tests for Apache Qpid.

The qpid-tests package has been upgraded to upstream version 0.10, which provides numerous improvements over the previous version. (BZ#675824)

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

1.237. qpid-tools

1.237.1. RHBA-2011:0774 — qpid-tools bug fix update

An updated qpid-tools package that fixes various bugs is now available for Red Hat Enterprise Linux 6.

The qpid-tools package provides management and diagnostic tools for Apache Qpid brokers and clients.

Bug Fixes

BZ#619353

When executing the "call %domainid create" command, the following error occurred:

```
        Exception in do_call: %r local variable 'smsg' referenced
before
assignment
```

This was caused by an uninitialized variable in the "do_call" method.

BZ#632678

The "list" command, provided by the qpid-tools package, did not show the "node" object in libvirt-qpid.

BZ#670956

QMFv2 supports map arguments, however, qpid-tools could not be used to call the methods that use the map arguments.

BZ#679803

The qpid-tools package has been upgraded to upstream version 0.10, which provides a number of bug fixes and enhancements over the previous version.

BZ#696195

Prior to this update, qpid-tools was not able to use the JobServer's "GetJobAd" call.

All users of qpid-tools are advised to upgrade to this updated package, which resolves these issues.

1.238. qt

1.238.1. RHSA-2011:1323 — Moderate: qt security update

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

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

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. HarfBuzz is an OpenType text shaping engine.

Security Fixes

CVE-2011-3193

A buffer overflow flaw was found in the harfbuzz module in Qt. If a user loaded a specially-crafted font file with an application linked against Qt, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

CVE-2011-3194

A buffer overflow flaw was found in the way Qt handled certain gray-scale image files. If a user loaded a specially-crafted gray-scale image file with an application linked against Qt, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of Qt should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications linked against Qt libraries must be restarted for this update to take effect.

1.238.2. RHSA-2011:1328 — Moderate: qt security update

Updated qt packages that fix two security issues are now available for Red Hat Enterprise Linux 6 FasTrack.

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

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. HarfBuzz is an OpenType text shaping engine.

Security Fixes

CVE-2011-3193

A buffer overflow flaw was found in the harfbuzz module in Qt. If a user loaded a specially-crafted font file with an application linked against Qt, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

CVE-2011-3194

A buffer overflow flaw was found in the way Qt handled certain gray-scale image files. If a user loaded a specially-crafted gray-scale image file with an application linked against Qt, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of Qt should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications linked against Qt libraries must be restarted for this update to take effect.

1.238.3. RHBA-2011:0314 — qt bug fix update

Updated qt packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System.

Bug Fixes

BZ#562049

In the Bengali script, a certain consonant conjunct with a zero-with joiner (that is, the "U+09B0 U+200D U+09CD U+09AF" sequence in Unicode) was not rendered correctly. This error has been fixed, and this conjunct is now rendered as expected.

BZ#562058

In the Bengali script, some character combinations were incorrectly rendered with an extra space between them (for example, the "U+0989 U+09CD U+09AA U+09BE U+09A6 U+09A8 U+09C7 U+09B0" sequence in Unicode). This update ensures that these combinations are correctly rendered with a straight line at the upper part of the text.

BZ#562060

In the Kannada script, the "U+0CB0 U+200D U+0CCD U+0C95" Unicode sequence produced an incorrectly rendered glyph. With this update, the underlying source code has been modified to address this issue, and the above glyph is now rendered properly.

BZ#631732

In the Marathi language, a certain combination of syllables (that is, the "U+0915 U+09EF U+09EF" sequence in Unicode) was not recognized properly. This update resolves this issue, and this combination is now rendered as expected.

BZ#636399

In the Oriya script, some character combinations (such as the "U+0B2C U+0B4D U+0B21" Unicode sequence) were not rendered correctly. With this update, a patch has been applied to address this issue, and such character combinations are now rendered correctly.

All users of Qt are advised to upgrade to these updated packages, which resolve these issues.

1.239. quota

1.239.1. RHBA-2011:0716 — quota bug fix and enhancement update

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

The quota utility provides system administration tools for monitoring and limiting user and group disk usage on file systems.

Bug Fixes

BZ#623656

Previously, quota utilities did not recognize the file system as having quotas enabled and refused to operate on it due to incorrect updating of /etc/mtab. This update prefers /proc/mounts to get a list of file systems with enabled quotas. Now, quota utilities recognize file systems with enabled quotas as expected.

BZ#662997

Previously, the manual pages for quota(1), edquota(8), and setquota(8) did not document the option "--always-resolve". This update adds this option to these manual pages.

BZ#663027

Previously, the default configuration of the warnquota tool incorrectly advised to inspect possible non-existing block devices and tried to check for non-existing or not-configured devices. This update changes the default content of /etc/quotatab.

BZ#667755

Previously, quota queries or limits for network-mounted file systems were not handled correctly if quota values were 2^32 or bigger. Due to this issue, values were not properly transported over RPC and interpreted by client. Mangled values (wrapped to 32 bits) were reported by the client. This update interprets the RPC values by the client correctly. Now, the block quota usage and limit values bigger than 2^32-1 are correctly reported by client.

BZ#668709

Previously, another value than the one specified was stored in the quota file when the quota limit was set to a value bigger than supported by the quota file format on file system with disabled quota enforcing. With this update, such settings are not anymore accepted.

BZ#668710

Previously, another value than the one specified was transmitted to the server and stored in the quota configuration when the quota limit was set to value 2^32 or bigger on an remote file system via RPC call. With this update, such settings are not anymore accepted.

BZ#684017

Previously, the support for vsfv1 quota format contained a memory leak when working with on-disk quota file. This update frees the memory correctly once it's not needed anymore. Now, memory leaks no longer occur.

BZ#688161

The repquota tool read data before synchronizing quota file with kernel. Prior to this update, the tool unexpectedly aborted on broken extended file system quota files. Now, repquota reads consistent quota files reflecting the latest state, the quota data for all users are reported as expected.

Enhancements

BZ#547748

This update allows for GFS2 file system quotas to be queried using quota utilities locally and via rpc.rquotad running on NFS server remotely.

BZ#609795, BZ#669598

With this update, the superuser can set block limits beyond 2^32-1 values if the file system utilizes the 64-bit quota format. For extended file systems, the quota format is called vfsv1 and must be explicitly enabled by mount options, e.g. mount -o jqfmt=vfsv1,usrjquota=aquota.user /dev/sdb1 /mnt/point.

BZ#634137

This update adds the new quota_nld system service to start the quota netlink daemon. The daemon listens to the kernel for disk quota excesses and notifies the user. The service can be configured in the /etc/sysconfig/quota_nld file.

BZ#658586

This update allows for GFS2 quotas to be explicitly synchronized with the new quotasync(1) utility and manipulated by quota utilities. Quota enforcement can be switched on and off at mount time or by remounting the file system (quota=on, quota=off mount options) only.

All quota users are advised to upgrade to this updated quota package, which fixes these bugs and adds these enhancements.

1.240. rds-tools

1.240.1. RHBA-2011:0754 — rds-tools bug fix and enhancement update

An updated rds-tools package that fixes bugs and provides enhancements is now available for Red Hat Enterprise Linux 6.

The rds-tools package provides a set of support tools for the Reliable Datagram Socket (RDS) protocol.

The rds-tools package has been upgraded to upstream version 2.0.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#636908)

Bug Fix

BZ#643113

Previously, the "rds-ping" command failed because the RDS protocol did not automatically enable the available underlying transports. This update adds a configuration file to the /etc/modprobe.d/ directory, and the transport modules are now loaded automatically whenever the main RDS module is loaded.

Users are advised to upgrade to this updated rds-tools package, which fixes these bugs and adds these enhancements.

1.241. Red Hat Enterprise Linux Release Notes

1.241.1. RHEA-2011:0728 — Red Hat Enterprise Linux 6.1 Release Notes

Updated packages containing the Release Notes for Red Hat Enterprise Linux 6.1 are now available.

These packages contain the Release Notes for Red Hat Enterprise Linux 6.1

1.242. redhat-lsb

1.242.1. RHBA-2011:0639 — redhat-lsb bug fix update

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

Linux Standards Base (LSB) provides a set of standards that increases compatibility among Linux distributions. The redhat-lsb package provides utilities needed for LSB compliant applications. It also contains requirements that ensure that all components required by LSB are installed on the system.

Bug Fix

BZ#585947

The redhat-lsb packages have been upgraded to comply with LSB version 4.0.

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

1.243. redhat-release

1.243.1. RHEA-2011:0540 — redhat-release enhancement update for Red Hat Enterprise Linux 6.1

An enhanced redhat-release package is now available for Red Hat Enterprise Linux 6.1.

The redhat-release package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

This updated redhat-release package reflects changes made for the release of Red Hat Enterprise Linux 6.1.

Users of Red Hat Enterprise Linux 6 are advised to upgrade to this updated redhat-release package, which adds this enhancement.

1.244. redhat-rpm-config

1.244.1. RHBA-2011:0763 — redhat-rpm-config bug fix and enhancement update

Updated redhat-rpm-config packages that fix a bug and add an enhancement are now available.

The redhat-rpm-config package provides various macro functions used in the production of RPMs. This updated package fixes a bug and adds an additional macro.

Bug Fix

BZ#627234

A typo existed in the code which affected the disabling of automatic build-time dependencies. This update fixes this.

An additional macro has been added:

BZ#658280

%kernel_module_package_moddir is a macro that abstracts the location of certain additional drivers on a system. This macro can be used by several different Linux distributions, including Red Hat Enterprise Linux.

All users should install this updated package, which fixes this bug and adds this enhancement.

1.245. report

1.245.1. RHBA-2011:0703 — report bug fix update

Updated report packages that address three bugs are now available for Red Hat Enterprise Linux 6.

The report packages contain a generic problem-, bug-, incident-, and error-reporting library, which can be configured to deliver a report to a variety of different ticketing systems.

Bug Fixes

BZ#624676

In some cases the report library failed to honor "target" options set in the "[main]" section of /etc/report.conf (the report configuration file). This presented as report asking for a target even when one was set in report.conf. With this update, report honors all options set in the configuration file, including targets set as part of the [main] section, as expected.

BZ#626994

Previously, when sending files to a Strata server along with the Strata case, the report library's Strata plug-in sent the files under their temporary name, rather than the original. This update corrects this and files sent to Strata servers are now sent with their original file names, as expected.

BZ#672647

The report spec file did not specify ISA (Instruction Set Architecture) specific dependencies. This could cause dependency-related problems if the report packages were ever downgraded. With this update the spec file includes ISA specific dependencies as required.

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

1.246. resource-agents

1.246.1. RHBA-2011:0744 — resource-agents bug fix and enhancement update

Updated resource-agents packages that provide fixes for various bugs and add enhancements 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 Fixes

BZ#631943

The Apache resource agent no longer errors out with "Query Failed" messages

BZ#633856

Error messages from the LVM resource agents now correctly appear in the system logs

BZ#639252

SAPInstance and SAPDatabase agents now work if /u exists

BZ#648897

The resource agent for named now works correctly

BZ#660337

migrate_uri support for virtual machine resources has been fixed

BZ#674710

Schema generation has been updated

BZ#669832

GFS2 reference handling has been fixed

BZ#683213

Mirror device failure during HA lvm service relocation may cause service failure

BZ#635828

AVC denials starting rpc.statd from the nfsserver resource agent have been addressed

Enhancements

BZ#621538

It is now possible to disable the use of rdisc by the ip resource agent

BZ#629275

Two new resource agents are provided which separate Oracle database instances from listeners. This feature is offered as a Technical Preview and is not recommended for production environments.

All users of the resource-agents package are advised to upgrade to these updated packages, which address these issues and add these enhancements.

1.247. rgmanager

1.247.1. RHBA-2011:0750 — rgmanager bug fix and enhancement update

An updated rgmanager package that provides bug fixes and adds enhancements is now available for Red Hat Enterprise Linux 6.

The rgmanager package contains the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

Bug Fixes

BZ#634298

clustat now correctly displays flags when a service is frozen or partially failed.

BZ#661881

clufindhostname -i no longer returns a random value.

BZ#621694

Restricted failover domain boundaries are now honored when performing virtual machine migrations.

BZ#621652

clustat no longer returns 255 if rgmanager is not running.

BZ#639103

The last owner field in "clustat -l" is now updated when a service fails over due to node death.

BZ#672841

Previously, if a service was in the "starting" state, failover domain rules would cause the service to relocate to a higher-priority node even if "nofailback" was set. This no longer occurs.

Enhancements

BZ#657756

rgmanager now sends signals to dbus when services change state.

BZ#634277

Independent subtrees may now be flagged as "non-critical," meaning they may fail and have their components manually restarted without the entire service being affected.

All users of rgmanager are advised to upgrade to this updated package, which addresses these issues and adds these enhancements.

1.247.2. RHBA-2011:0960 — rgmanager bug fix update

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

The rgmanager package contains the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

Bug Fix

BZ#721004

Prior to this update, any resource agent returning corrupted or invalid metadata would cause the rgmanager utility to terminate unexpectedly and the node to be fenced. With this update, rgmanager is able to skip the broken agent and continue operating as expected, thus fixing this bug.

Users of rgmanager are advised to upgrade to this updated package, which fixes this bug.

1.248. rhn-client-tools

1.248.1. RHBA-2011:0565 — rhn-client-tools bug fix and enhancement update

Updated rhn-client-tools and yum-rhn-plugin packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The rhn-client-tools and yum-rhn-plugin packages provide programs and libraries that allow a system to receive software updates from Red Hat Network (RHN) and Red Hat Network Satellite.

Bug Fixes

BZ#580479

Prior to this update, the graphical user interface of the **firstboot** application did not allow a user to select the EUS (Extended Update Support) channel during the configuration of software updates. With this update, the **firstboot** application has been adapted to include the **`Select operating system release`** screen. Now, when the EUS channel is available for the system, users are now allowed to select it from the pulldown list.

BZ#581482

Previously, the **rhn_register** utility for the graphical user interface and its variant for the text user interface (started by using the **rhn_register --nox** command) used different names for various window titles and buttons. This update corrects these inconsistencies, and both variants of **rhn_register** now share the same window titles and button labels.

BZ#596108

When using the graphical version of the **firstboot** application to configure software updates, clicking the **Back** button on the **Review Subscription** screen and then clicking **Forward** caused the system to be registered twice, consuming two entitlements. With this update, the **firstboot** application has been adapted to prevent multiple system registrations. Now, clicking the **Back** button on the **Review Subscription** screen leads a user back to the **Set Up Software Updates** screen, which no longer allows the user to register the system when it is already registered.

BZ#602609

Under certain circumstances, lines similar to the following may have been written to standard error when running the **rhn_register** utility in the graphical user interface:

```
/usr/share/rhn/up2date_client/messageWindow.py:72: DeprecationWarning:
use set_markup() instead
```

This update adapts the **rhn_register** not to produce these messages.

BZ#606222

When using the **firstboot** application to configure software updates, the **Choose Server** screen did not allow users to use keyboard for navigation. This was caused by a label incorrectly getting the focus. With this update, the underlying source code has been adapted to remove the focus from the label, and users are now able to use the keyboard for navigation as expected.

BZ#617066

When using the Malayalam translation (that is, the **ml_IN** language code) of the **firstboot** application to configure software updates, the **Why Register** dialog box may have been too long to fit to the screen on certain display resolutions (that is, with height 600px and smaller). This update extends the width of the dialog box to ensure it fits to the screen as expected.

BZ#621138

Due to a different format of **/proc/cpuinfo** on IBM System z machines, Red Hat Network Client Tools may have reported an incorrect number of CPUs on this platform. This update adapts the underlying source code to ensure that the correct number of CPUs is reported on IBM System z machines.

BZ#625791

When the **networkRetries** configuration option in the **/etc/sysconfig/rhn/up2date** file was set to a non-integer value, network operations of the registration tools did not time out at all. With this update, the registration tools correctly set the default value of **networkRetries** to **1**, and invalid values are now interpreted as a single attempt. As a result, network operations now time out as expected.

BZ#626752

When registering a system, previous versions of Red Hat Network Client Tools failed to recognize a

fully-virtualized Red Hat Enterprise Linux 6 Xen guest, and incorrectly listed it as a paravirtualized guest. This update ensures that Red Hat Network Client Tools now recognize the virtualization type of fully-virtualized Red Hat Enterprise Linux 6 Xen guests correctly.

BZ#627525

Previously, enabling the **rhnplugin** Yum plug-in rendered the **tsflags** plug-in unusable, and an attempt to run the **`yum install --tsflags`** command failed with the following error:

```
Command line error: no such option: --tsflags
```

This update corrects this error, and the **rhnplugin** and **tsflags** plug-ins can now be used together as expected.

BZ#630575

When running the **firstboot** application in the Oriya language (that is, the **`or_IN`** language code), the **`No thanks, I'll connect later`** button did not have any shortcut key assigned to it. With this update, the button is now associated with the **`N`** key.

BZ#632282

Previously, the **rhn_register** utility for the graphical user interface did not honor the **`hostedWhitelist`** option in the **`/etc/sysconfig/rhn/up2date`** configuration file. This update corrects this error, and **rhn_register** now uses this option as expected.

BZ#634835

Due to incorrect use of HTML entities in the Russian translation (that is, the **`ru_RU`** language code) of the **firstboot** application, various screens regarding the configuration of software updates contained HTML tags, such as **** or ****. This update replaces these entities with plain text, and the Russian translation of **firstboot** is now displayed correctly.

BZ#638982

This update ensures that System Management BIOS (SMBIOS) data are properly encoded before they are sent over the **`XML-RPC`** protocol.

BZ#649233

When running the **rhn_register** utility for the graphical user interface, clicking the **`Back`** button after a failed attempt to provide a short password caused the mouse pointer to remain busy. This error has been fixed, and the mouse pointer is now properly restored.

BZ#651403

Previously, the **`Select operating system release`** screen of the **rhn_register** utility for the graphical user interface incorrectly referred to Red Hat Enterprise Linux 5, even when Red Hat Enterprise Linux 6 was used. With this update, this error no longer occurs, and the utility now correctly refers to the correct version of Red Hat Enterprise Linux.

BZ#651777

Previously, the manual page for the **rhn-channel** utility was missing. This update adds the **rhn-channel**(8) manual page as a symbolic link to **spacewalk-channel**(8).

BZ#651789

Prior to this update, the **spacewalk-channel** utility incorrectly reported success even when an attempt to add or remove a wrong channel failed. With this update, adding or removing a wrong channel now causes **spacewalk-channel** to report an error as expected.

BZ#651857

Prior to this update, certain combinations of command line options may have caused the **spacewalk-channel** utility to terminate unexpectedly with a traceback written to standard error. With this update, the underlying source code has been adapted to address this issue, and all supported command line options now work as expected.

BZ#652424

This update re-includes the `useNoSSLForPackages` option in the `/etc/sysconfig/rhn/up2date` configuration file. When enabled (that is, when set to `1`), this option forces the use of the HTTP protocol for downloading repository metadata and RPM packages. Note that enabling this option *disables* Location-Aware Updates.

BZ#656380

In order to allow communication with multihomed Red Hat Network Proxy Servers over the HTTPS protocol, a previous version of the **rhnplugin** Yum plug-in disabled the SSL server name check for XML-RPC communication. For security reasons, the SSL server name check for the XML-RPC communication is no longer disabled.

BZ#666463

Due to **rhnplugin** not respecting Yum's `metadata_expire` configuration option, all channels used the default expiration time of 6 hours. This update adapts **rhnplugin** to use Yum's global settings.

BZ#666545

Prior to this update, when an outdated cache prevented the **rhn_check** utility from finding package information, the utility incorrectly reported success. This update adapts **rhn_check** to report failure in these situations.

BZ#666860

Prior to this update, the **firstboot** application always prompted a user to register the system with RHN Classic (previously named Red Hat Network). With this update, **firstboot** no longer prompts users to register their system with RHN Classic when they choose to register using the RHN Certificate-Based Entitlement technology.

BZ#667739

Various parts of the underlying source code have been adapted to make it easier to use the **rhn_register** utility with assistive technologies.

BZ#671032, BZ#671041

The **rhn_register** and **rhnreg_ks** utilities, the **rhnplugin** Yum plug-in, and their corresponding manual pages have been updated to reflect the change of the name from Red Hat Network to RHN Classic.

BZ#672471

When a system was not registered with RHN Classic or Red Hat Network Satellite Server, an attempt to remove a package by using the `yum remove` command failed, and a traceback was written to standard error. This was caused by **rhnplugin** incorrectly sending the list of removed packages to a

Red Hat Network server. This update adapts **rhnplugin** not to send the list to a server when a system is not registered, and the **yum remove** command now works as expected.

BZ#679217

The **firstboot** application has been updated to mention the RHN Certificate-Based Entitlement technology as an alternative to RHN Classic.

BZ#680124

When gathering hardware information, previous versions of the **rhn_register** utility only submitted the number of active CPUs. However, especially on IBM System z systems, this value may vary over time. With this update, the **rhn_register** utility has been adapted to parse **/sys/devices/system/cpu** instead of **/proc/cpuinfo**, which reports all present CPUs.

BZ#684245

When using a non-English translation of the **firstboot** application, an attempt to register a system using the RHN Certificate-Based Entitlement technology failed, and a traceback was written to standard error. This was caused by a difference in the translation of the subscription-manager and rhn-client-tools packages. This error has been fixed, and the relevant part of the **firstboot** application no longer depends on a particular translation.

BZ#684248

Due to an incorrect binding to a wrong **gettext** domain, various parts of the **firstboot** application and the **rhn_register** utility were not translated. This error no longer occurs, and both programs are now translated as expected.

BZ#688870

Previously, the presence of an unknown channel name in the **/var/cache/yum/rhnplugin.repos** file caused certain Yum commands to fail with the following error:

```
Error: Cannot retrieve repository metadata (repomd.xml) for repository:
repository_name. Please verify its path and try again
```

With this update, the **rhnplugin** has been adapted to ensure that such an error no longer prevents Yum from finishing.

BZ#690234

Under certain circumstances, the **yum groupinstall** command may have failed to install the selected package group with the following result:

```
No packages in any requested group available to install or update
```

This was caused by the Yum cache being populated twice. This update fixes this error, and the **yum groupinstall** command now works as expected.

BZ#691188

Prior to this update, an attempt to use an invalid SSL certificate for communication with RHN Classic or Red Hat Network Satellite Server caused **Yum** to terminate unexpectedly with a traceback. This update adapts the **rhnplugin** Yum plug-in to raise an exception in this case, and both Yum and the tools for the graphical user interface now display a proper error message.

BZ#697835

Previously, an attempt to run the **`rhnreg_ks --help`** command in a non-English environment may have failed with a traceback written to standard error. This was caused by the presence of a non-ASCII character in translated strings. With this update, the underlying source code has been adapted to retrieve the strings in Unicode, and running the **rhnreg_ks** utility with the **`--help`** option no longer causes it to crash.

Enhancements

BZ#626739

This update adds support for the Red Hat Network Satellite Server Maintenance Window. This allows users to download scheduled packages and errata before the start of a maintenance window. Note that this option is *disabled* by default. For information on how to enable it, refer to https://access.redhat.com/site/solutions/42227.

BZ#651792

The **spacewalk-channel** utility now supports the **`-L`** (or **`--available-channels`**) option, which allows a user to list all available child channels that are related to a system.

BZ#662704

The comment for the **`serverURL`** option in the **`/etc/sysconfig/rhn/up2date`** configuration file has been updated to mention that a *fully qualified domain name* (FQDN) must be specified.

BZ#671039

When a user attempts to register a system with RHN Classic and the system is already subscribed using the RHN Certificate-Based Entitlement technology, the **rhn_register** utility now displays a warning that the system is already registered using a different method.

All users of rhn-client-tools and yum-rhn-plugin are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.249. rhnlib

1.249.1. RHEA-2011:0798 — rhnlib enhancement update

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

The rhnlib package consists of a collection of Python modules used by the Red Hat Network (RHN) software.

Enhancement

BZ#684815

This update introduces two new functions which add support for upcoming Internationalized Domain Name (IDN) in future releases of yum-rhn-plugin, RHN Tools and RHN Satellite.

Users of rhnlib are advised to upgrade to this updated package, which adds this enhancement.

1.250. ricci

1.250.1. RHBA-2011:0749 — ricci bug-fix update

Updated ricci packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

The ricci packages contain a daemon and a client which allow a cluster to be configured and managed remotely.

Bug Fixes

BZ#652837

Ricci no longer sends non-SSL data when it has reached its maximum number of connections.

BZ#644047

Ricci no longer depends on the root user password to permit access; authentication is now done using the ricci user password.

BZ#614647

Ricci can now be configured remotely using ccs.

BZ#623734

Nodes can now be started and stopped using ccs.

BZ#602399

A man page has been added for ricci.

BZ#682317

It is now possible to pipe passwords into ccs_sync.

BZ#682868

ccs now fails (with an error) if a non-validating cluster.conf file is used.

BZ#682323

When an incorrect password is entered for a node in ccs_sync, it no longer continues to ask for the password in an endless loop.

All users of ricci are advised to upgrade to these updated packages, which address these issues.

1.250.2. RHBA-2011:1235 — ricci bug-fix update

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

The ricci (remote configuration interface) packages contain a daemon and a client which allow a cluster to be configured and managed remotely.

Bug Fix

BZ#732616

The fencing agent for Cisco UCS, included in the Red Hat Enterprise Linux 6.1 cluster, supports the "suborg" option. However, this option was not defined in the schema for the /etc/cluster/cluster.conf file. As a consequence, utilities such as ccs returned error messages about the schema violation at the attempt to define fencing for UCS blade servers with the "suborg" option, and the fenced daemon

did not start if this definition was forced into the cluster configuration file. With this update, a patch that adds the "suborg" option to the cluster configuration schema definition for the fence_cisco_ucs agent has been provided, thus fixing this bug.

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

1.251. rng-tools

1.251.1. RHEA-2011:1464 — rng-tools enhancement update

An enhanced rng-tools package that adds two enhancements is now available for Red Hat Enterprise Linux 6.

The rng-tools package contains the random number generator user space utilities, such as the rngd daemon.

Enhancements

BZ#749183

A new "-i, --ignorefail" command line option has been added to the rngd daemon. This option allows rngd to ignore repeated warning messages about failed FIPS checks.

BZ#751356

The rngd(8) manual page has been modified to include the "-i, --ignorefail" option.

All users of rng-tools are advised to upgrade to this updated package, which adds these enhancements.

1.252. rpm

1.252.1. RHSA-2011:1349 — Important: rpm security update

Updated rpm packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6, and Red Hat Enterprise Linux 3 Extended Life Cycle Support, 5.3 Long Life, 5.6 Extended Update Support, and 6.0 Extended Update Support.

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

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Security Fix

CVE-2011-3378

Multiple flaws were found in the way the RPM library parsed package headers. An attacker could create a specially-crafted RPM package that, when queried or installed, would cause rpm to crash or, potentially, execute arbitrary code.

Note: Although an RPM package can, by design, execute arbitrary code when installed, this issue would allow a specially-crafted RPM package to execute arbitrary code before its digital signature has been verified. Package downloads from the Red Hat Network remain secure due to certificate

checks performed on the secure connection.

All RPM users should upgrade to these updated packages, which contain a backported patch to correct these issues. All running applications linked against the RPM library must be restarted for this update to take effect.

1.252.2. RHBA-2011:0739 — rpm bug fix and enhancement update

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

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Bug Fixes

BZ#479608, BZ#553108

The "freshen" (rpm -F/--freshen) operation did not consider the architecture of a system when selecting update candidates, which caused either misleading error messages or packages being updated to a different architecture inappropriately on multilib systems. RPM now requires an exact architecture match between packages on multilib systems to perform the freshen operation.

BZ#565843

RPM previously forced the umask of a process to "022" at library initialization, which could cause unwanted behavior for API users, especially in python, where importing the rpm module would silently change the umask. The umask is now only changed for the duration of a transaction and restored to its previous value afterwards.

BZ#607222

Package signing could result in a misleading passphrase-related error message when the passphrase was correct but other issues (such as an expired key) prevented signing. Since RPM relies on GnuPG to perform package-signing, it has no knowledge of such details and cannot report them. However, to avoid this situation, any error messages from GnuPG are now passed to RPM users where they were previously silenced unless verbose mode was used when signing packages.

BZ#608599

Using custom signing parameters such as a different digest algorithm, it was possible to successfully sign a package that RPM could not validate due to differencies in supported algorithms between GnuPG and NSS. RPM now gives an error message when unsupported parameters are used in package signing.

BZ#608608, BZ#681013

Package (re)signing could lead to multiple bad signatures being added to a package, rather than being replaced appropriately, because of flawed heuristics used in determining the signature type. Pre-existing and newly created signatures are now compared in detail to precisely determine the need to replace or skip signatures.

BZ#609117

Attempting to build packages that contained fonts when the fontconfig package was not installed sometimes led to the build failing with a "getOutputFrom(): Broken pipe" error because of flaws in the dependency generation system. The "font provides" helper script now always flushes stdin to prevent

this from occurring. Additionally, the error message has been made more informative to make catching such issues easier in the future.

BZ#668629

Attempting to verify packages with "%verifyscript" caused the script to run twice and fail to reflect a failure in response to an RPM exit code. These were simple logic errors, which have been fixed in this update.

BZ#680261

When both the primary and secondary architecture versions of a package were installed and then updated or erased, RPM failed to erase all files of the previous installation because erasure order was incorrect in cases where order was not dictated by other dependencies. Erasure ordering between primary and secondary architecture packages is now handled correctly in this situation.

BZ#618428

debuginfo generation could fail to handle cross-directory hard links between binaries in some rare situations, causing corresponding .debug files to be missing in the generated package. This update ensures cross-directory hard linked files in packages are always handled correctly during debuginfo generation.

Enhancement

BZ#652787

debuginfo generation has been enhanced to generate pre-calculated index files for the GNU Project Debugger (gdb). These indexes improve gdb startup times.

All users of the RPM Package Manager are advised to upgrade to these updated packages, which correct these issues and add this enhancement.

1.253. rsyslog

1.253.1. RHSA-2011:1247 — Moderate: rsyslog security update

Updated rsyslog 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 rsyslog packages provide an enhanced, multi-threaded syslog daemon that supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grained output format control.

Security Fix

CVE-2011-3200

A two byte buffer overflow flaw was found in the rsyslog daemon's parseLegacySyslogMsg function. An attacker able to submit log messages to rsyslogd could use this flaw to crash the daemon.

All rsyslog users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, the rsyslog daemon will be restarted automatically.

1.253.2. RHBA-2011:0785 — rsyslog enhancement update

Enhanced rsyslog packages are now available for Red Hat Enterprise Linux 6.

The rsyslog packages provide an enhanced, multi-threaded syslog daemon that supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. Rsyslog is compatible with stock sysklogd, and can be used as a drop-in replacement. It is simple to set up, with advanced features suitable for enterprise-class, encryption-protected syslog relay chains.

Enhancement

BZ#642994

With this update, rsyslog is built with the PIE (Position Independent Executable) and RELRO (read-only relocations) flags, thus, increasing the overall security. Also, rsyslog now owns the "/etc/pki/rsyslog" directory. A ChangeLog which contains a record of changes made to the rsyslog package was added to the existing documentation in the "/usr/share/doc/rsyslog-[VERSION]" directory.

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

1.253.3. RHEA-2011:1358 — rsyslog enhancement update

Updated rsyslog packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The rsyslog packages provide an enhanced, multi-threaded syslog daemon that supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grained output format control.

BZ#742275

This update introduces the new configuration option "SpaceLFOnReceive" and the log format template "RSYSLOG_SysklogdFileFormat". These new features allow users to configure rsyslog to behave like the old sysklogd daemon, available in previous releases.

Users that require sysklogd compatibility from rsyslog are advised to upgrade to these updated rsyslog packages, which add this enhancement.

1.253.4. RHBA-2011:0936 — rsyslog bug fix update

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

The rsyslog packages provide an enhanced, multi-threaded syslog daemon that supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grained output format control.

Bug Fix

Prior to this update, the "$ActionSendStreamDriverMode" configuration directive did not have any effect on big-endian platforms. Due to this behavior, the Transport Layer Security (TLS) encryption was not enabled. This update modifies the code to correctly process the configuration directive. Now, TLS encryption works as expected.

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

1.254. ruby

1.254.1. RHSA-2011:0910 — Moderate: ruby security update

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

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

Security Fixes

CVE-2011-0188

A flaw was found in the way large amounts of memory were allocated on 64-bit systems when using the BigDecimal class. A context-dependent attacker could use this flaw to cause memory corruption, causing a Ruby application that uses the BigDecimal class to crash or, possibly, execute arbitrary code. This issue did not affect 32-bit systems.

CVE-2011-1004

A race condition flaw was found in the remove system entries method in the FileUtils module. If a local user ran a Ruby script that uses this method, a local attacker could use this flaw to delete arbitrary files and directories accessible to that user via a symbolic link attack.

CVE-2011-1005

A flaw was found in the method for translating an exception message into a string in the Exception class. A remote attacker could use this flaw to bypass safe level 4 restrictions, allowing untrusted (tainted) code to modify arbitrary, trusted (untainted) strings, which safe level 4 restrictions would otherwise prevent.

Red Hat would like to thank Drew Yao of Apple Product Security for reporting the CVE-2011-0188 issue.

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

1.254.2. RHBA-2011:0721 — ruby bug fix update

Updated ruby packages that fix several bugs 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 perform system management tasks.

Bug Fixes

BZ#635588

Previously, Ruby's self-test failed because of a false-positive. The erroneous result has been corrected and the test no longer fails.

BZ#635588

Ruby's self-test failed because of a bug in GNU dbm (gdbm). Until this bug is corrected, the test is omitted from Ruby's self-test to avoid this failure.

All users of Ruby are advised to upgrade to these updated packages, which correct these bugs.

1.255. s390utils

1.255.1. RHBA-2011:0601 — s390utils bug fix update

An updated s390utils package that fixes multiple bugs and adds some enhancements is now available for Red Hat Enterprise Linux 6.

The s390utils package contains utilities related to Linux for the IBM System z architecture.

Enhacements for the libzfcphbaapi subpackage:

BZ#633409

This updated package provides two new tools:

- **zfcp_ping** — attempts to verify the existence of a destination by sending a request and waiting for a reply.
- **zfcp_show** — provides information about a connected SAN, including interconnect elements, the number and status of ports, and a potentially connected node port.

BZ#633414

The **`lib-zfcp-hbaapi`** library provided by this package is rebased to version 2.1.

Enhancements and bug fixes in s390utils itself:

BZ#631541, BZ#631561

This updated package provides three new tools:

- **hyptop** — a dynamic of a System z hypervisor environment in real time.
- **lsmem** — lists the ranges of available memory and their status, whether online or offline.
- **chmem** — sets a particular size or range of memory online or offline.

BZ#631546

The s390-tools package now provides **cmsfs-fuse**, a tool that can mount a CMS disk as a writeable file system using the **FUSE** infrastructure on Linux. This new tool allows you to read and write configuration files on CMS disks directly.

BZ#597360

Previously, the wrong control unit type for CTC devices was used in the **udev** rules. As a result, CTC devices were not being detected. In this updated package, the rules are corrected and devices are detected properly on system startup.

BZ#619504

Previously, the **xcec-bridge** utility did not process link-level headers in incoming packets. The utility therefore could not forward multicast network traffic. Now, **xcec-bridge** are taken in to account and multicast forwarding works.

BZ#623250

When the **ziomon** command exits successfully, it should return a value of **0**. Previously, faulty logic caused the command to return an exit status of **1** when run with the **--help** or **-v** arguments. The logic is now corrected and **ziomon** returns **0** when run successfully with **--help** or **-v**.

BZ#627692

Previously, the code used by **qethconf** to process devices assumed that the device subchannel was set to **0**. Consequently, devices where the subchannel was set to any other value were not processed and did not appear on the IPA list. Now, **qethconf** recognizes devices where the subchannel is set to values other than **0** and these devices appear correctly in the IPA list.

BZ#631527

The **cio_settle** kernel facility is a new mechanism by which processes in user space can monitor CIO actions. Previously, user-space processes could not wait for devices to become available, leading to possible race conditions, particularly as the system started and started processing CIO requests. This updated s390-utils package uses this mechanism to enable user space processes to wait for devices to become usable. Now that processes can wait for device availability, handling of all CIO actions is ensured and race conditions are avoided.

BZ#633411, BZ#676706

Previously, triggering a dump too soon after a kernel panic could lead to an infinite panic–dump–IPL loop. This updated package introduces ***DELAY_MINUTES*** as a new keyword for the **etc/sysconfig/dumpconf** configuration file, and updates the **dumpconf** manual page to describe its use. When configured, the new keyword delays the dump and therefore help to avoid situations where triggering the dump leads to a re-IPL loop.

BZ#633420

Linux on System z might not provide a particular terminal or console. This updated package provides a new tool, **ttyrun**, which safely starts **getty** programs and prevents re-spawns through the init program if a terminal is not available.

BZ#633437

Previously, the **zfcpdump** utility could only read and write s390 format dumps. This updated package adds two new dump formats: ELF (source/target) and LKCD (target). Therefore the tool can now read ELF, s390 and LKCD and write ELF and s390 format dumps, allowing it to be used for dump format conversion. The ELF target format can be used to run the **makedumpfile** tool as a second step to compress the dump.

BZ#633534, BZ#636849

OSX and OSM are new network interface types from zEnterprise for hybrid data (management) networking. Previously, **znetconf** did not handle OSX and OSM devices, and could not be used to configure them. This updated package updates the tool's internal tables so that **znetconf** handles these devices correctly. Additionally, new **udev** rules ensure that these devices come up when the system starts.

BZ#636204

Previously, **iucvtty** passed the z/VM user ID of the originating guest virtual machine as an argument to the **-h** option of the **login** program. Depending on the implementation of the login program, passing the user ID to **login -h** can cause timeouts when the target system does not have a working network connection. Now **iucvtty** no longer passes the user ID and therefore avoids timing out during login.

BZ#644935

This updated package adds **-Q** as a new option to the **tunedasd** tool that allows it to show the reservation status of a given DASD in relation to the current Linux instance. Used on the command line, **tunedasd -Q** returns the reservation status to standard out.

BZ#649787

Previously, the **format 7** label written by **fdasd** and **dasdfmt** was incorrect. Therefore, backups of Linux on System z disks from z/OS did not work when the disk was not fully partitioned. **libvtoc** now writes the **format 7** label correctly and backups work correctly.

BZ#651012

Previously, the **cmsfs** utilities crashed when they were used on filesystems with block sizes different from the underlying device. Users had to work around the issue by creating a filesystem with the same block size as the device. With this updated package, **cmsfs** utilities report the mismatch in block sizes but still work.

BZ#658517, BZ#693365

Previously, **cpuplugd** contained incorrect checks. Therefore, when **cpuplugd** exited, it restored **/proc/sys/vm/cmm_pages** to **0**, regardless of its previous value. Also, when where ***cmm_pages*** was equal to ***cmm_inc***, **cmm_pages** did not correctly reach a ***cmm_min*** of **0** during run-time. The incorrect checks in the **cpuplugd** utility are now fixed, so that **/proc/sys/vm/cmm_pages** maintains its correct value, and the evaluation of ***cmm_min*** is now correct.

BZ#659828

Previously **lsluns** failed to report LUNs from the SAN Volume Controller (SVC). The strategy of **lsluns** is now changed to check if **LUN 0** or the **WLUN** is already available. If both LUNs are not available, **LUN 0** is tried first; if this fails, **WLUN** is tried.

BZ#660361

Previously **lsluns** did not accept uppercase letters for hex digits in the FCP device or WWPN. With this update, **lsluns** accepts uppercase and lowercase letters.

BZ#688140

The **mon_statd** script contained a call to **udevsettle** instead of **udevadm settle**, which failed because **udevsettle** doesn't exist. The call is now corrected and **mon_statd** works correctly.

BZ#688340

Previously, when **fdasd** tried to write to an read-only disk, it would attempt to format an error message through **libvtoc**, where it would cause a buffer overflow. Therefore, rather than a useful error message, users were presented with an error about a buffer overflow. The **fdasd** tool now prints the error message directly and therefore avoids the buffer overflow.

IBM System z users should install this updated package which addresses these issues and adds these enhancements.

1.256. samba

1.256.1. RHSA-2011:1221 — Moderate: samba and cifs-utils security and bug fix update

Updated samba and cifs-utils 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Samba is a suite of programs used by machines to share files, printers, and other information. The cifs-utils package contains utilities for mounting and managing CIFS (Common Internet File System) shares.

Security Fixes

CVE-2011-2694

A cross-site scripting (XSS) flaw was found in the password change page of the Samba Web Administration Tool (SWAT). If a remote attacker could trick a user, who was logged into the SWAT interface, into visiting a specially-crafted URL, it would lead to arbitrary web script execution in the context of the user's SWAT session.

CVE-2011-2522

It was found that SWAT web pages did not protect against Cross-Site Request Forgery (CSRF) attacks. If a remote attacker could trick a user, who was logged into the SWAT interface, into visiting a specially-crafted URL, the attacker could perform Samba configuration changes with the privileges of the logged in user.

CVE-2011-2724

It was found that the fix for CVE-2010-0547, provided in the cifs-utils package included in the GA release of Red Hat Enterprise Linux 6, was incomplete. The mount.cifs tool did not properly handle share or directory names containing a newline character, allowing a local attacker to corrupt the mtab (mounted file systems table) file via a specially-crafted CIFS share mount request, if mount.cifs had the setuid bit set.

CVE-2011-1678

It was found that the mount.cifs tool did not handle certain errors correctly when updating the mtab file. If mount.cifs had the setuid bit set, a local attacker could corrupt the mtab file by setting a small file size limit before running mount.cifs.

Note: mount.cifs from the cifs-utils package distributed by Red Hat does not have the setuid bit set. We recommend that administrators do not manually set the setuid bit for mount.cifs.

Red Hat would like to thank the Samba project for reporting CVE-2011-2694 and CVE-2011-2522, and Dan Rosenberg for reporting CVE-2011-1678. Upstream acknowledges Nobuhiro Tsuji of NTT DATA Security Corporation as the original reporter of CVE-2011-2694, and Yoshihiro Ishikawa of LAC Co., Ltd. as the original reporter of CVE-2011-2522.

Bug Fix

BZ#728517

If plain text passwords were used ("encrypt passwords = no" in "/etc/samba/smb.conf"), Samba clients running the Windows XP or Windows Server 2003 operating system may not have been able to access Samba shares after installing the Microsoft Security Bulletin MS11-043. This update corrects this issue, allowing such clients to use plain text passwords to access Samba shares.

Users of samba and cifs-utils are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the smb service will be restarted automatically.

1.256.2. RHBA-2011:0582 — samba bug fix update

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

Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers).

Bug Fixes

BZ#660667

The samba packages have been upgraded to the latest upstream version 3.5.6, which provides a number of bug fixes over the previous version.

BZ#654426, BZ#617614

Previously, when a user tried to copy a file larger than 16KB to a folder shared on the **Samba** network file system with **gvfs-copy**, an "Invalid argument" error message appeared while copying the file. This was caused by the SMB Signature verification failure during data transmission. The problem has been fixed so that files can now be copied successfully.

BZ#628955

Previously, the TPS Verify Test failed for **Samba**. This failure has been resolved so that **Samba** now passes the TPS Verify Test.

BZ#629374

Previously, **Samba** changed attributes on file rename. This unintended behavior has been fixed so that **Samba** no longer changes file attributes on file rename when it is not expected to.

BZ#640888

Previously, when a user configured a printer to be used in **Samba** with the **system-config-printer** configuration utility, it was not possible to successfully run the **cupsaddsmb** command using the Adobe Postscript Driver. Running the command resulted in the "WERR_UNKNOWN_PRINTER_DRIVER" error message. The problem has been fixed so that the **cupsaddsmb** command can now be executed successfully without the error.

BZ#641368

The **/etc/rc.d/init.d/nmb** startup script contained an erroneous description saying that it started **Samba**'s **smbd** service. In fact, the **nmb** script starts the **nmbd** service, which communicates with **NetBIOS** name service requests. This update corrects the description in the **nmb** startup script.

BZ#645173

Previously, when a domain user was added to a local group on a joined Windows workstation in **Samba**, a domain-joined machine failed to find other users. The issue has been resolved so that domain-joined machines are now able to find other users.

BZ#650244

Previously, there was a problem in that file names with characters encoded in ISO-8859-15 on the **Samba** network file system with UTF-8 configured as **`unix charset`** and **`display charset`** in the **`smb.conf`** configuration file were not displayed correctly while a user browsed the network file system with the **Windows Explorer** application. This has been fixed so that file names with characters encoded in ISO-8859-15 are now displayed without any character encoding problems on the **Samba** network file system.

BZ#650245

Previously, there was a problem with the limit of client connections in the **Samba** **`winbindd`** daemon. The limit was hard coded to the number of 200 connections, thus disallowing any other **`winbindd`** clients that would exceed the limit to connect. A fix resolving this bug has been applied so that it is now possible to exceed the original limit. The limit can now be set by modifying the **`winbind max clients`** option.

BZ#651947

Previously, when a user tried to connect to a Windows client with the **smbclient** utility, which is included in **Samba**, and there was at least one of the **Windows Live Essentials** programs installed on that Windows client, it was not possible to properly establish the connection. An error message appeared on the screen, stating "SPNEGO login failed: Invalid parameter". The problem has been fixed so that a user is now able to make a connection using the **smbclient** utility without getting any error.

BZ#667675

Previously, when a user tried to mount a **Samba** share using Kerberos 5 authentication, an input/output error was triggered and the user was unable to proceed with **Samba** share mounting. The fix for this problem has been provided in the **smbclient** utility so that share mounting with Kerberos 5 authentication works properly now.

BZ#596345

Previously, there was a typo in the **`smb.conf`** configuration file, which is included in **Samba**. The name of the **SELinux** label **`samba_share_t`** that a user uses when creating a new directory was misspelled as **`samba-share_t`**. The typo has been corrected and the **`smb.conf`** file now contains valid information.

BZ#626473

Previously, the **`smb.conf`** configuration file, which is included in **Samba**, misspelled the words "Network" and "Security". The misspellings have been corrected so that the content of the **`smb.conf`** file is now spelled properly.

BZ#629396

Previously, **Samba** was shipped with a manual page for the **winbind_krb5_locator** plug-in, but not with the plug-in itself. This issue has been resolved by including the missing **winbind_krb5_locator** plug-in in **Samba**.

BZ#639141

The description of the ***`default case`*** parameter in the **`smb.conf`** configuration file was unclear and contained misleading punctuation. This update clarifies the description so that it is unambiguous.

Enhancements

BZ#659884

This release introduces a significant improvement in **Samba** performance when writing large files on the ext3, ext4, or xfs file system. The performance improvement has been made possible by using the **`posix_fallocate()`** function in write paths.

BZ#560893

This update includes an improvement in that non-root users are now able to change their passwords in **Samba** when the **`smb.conf`** configuration file is configured in ADS (Active Directory Service) mode. This was not possible with the previous version of the **smbpasswd Samba** utility. The **`smbd`** daemon must run in order to change non-root user passwords with **smbpasswd** successfully. Also, with the **`wbinfo --change-user-password`** command, non-root users can now change both the local user password as well as the remote Active Directory domain password at the same time.

BZ#614853

Previously, a user checked the sanity of the **`smb.conf`** Samba configuration file with the **testparm** utility. The utility was not user-friendly in that its usage was not consistent with the way the sanity check has been called and performed in other similar packages like postfix. This has been improved by adding a new option **`configtest`** to the **`service smb`** command.

All users requiring Samba should install these newly released packages, which resolve these issues and add these enhancements.

1.257. saslwrapper

1.257.1. RHBA-2011:0809 — saslwrapper bug fix update

Updated saslwrapper packages that resolve an issue are now available for Red Hat Enterprise Linux 6.

The saslwrapper package contains Ruby and Python wrappers for the cyrus sasl library.

The saslwrapper package has been upgraded to upstream version 0.10, which provides numerous improvements over the previous version. (BZ#693862)

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

1.258. screen

1.258.1. RHBA-2011:0678 — screen bug fix update

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

The screen utility allows multiple logins on a single terminal. This is especially useful for users who telnet into a machine or are connected using a terminal that does not provide this functionality, but want to use more than one login.

Bug Fix

BZ#665103

Due to several unrelated bugs, the screen utility did not pass the Common Criteria certification requirements. This update modifies various parts of the underlying source code to address these issues.

All users of screen are advised to upgrade to this updated package, which resolves this issue.

1.259. scsi-target-utils

1.259.1. RHBA-2011:0734 — scsi-target-utils bug fix and enhancement update

An updated scsi-target-utils package that fixes multiple bugs and adds an enhancement is now available.

The scsi-target-utils package contains tools and a daemon used to set up iSCSI and iSER targets.

Bug Fix

BZ#676337

Providing an existing target name to tgt-setup-lun when attempting to add a new LUN based on a non-existent device correctly resulted in failure because a target with the same name already existed. If the user then followed the utility's suggestion to add the new LUN to the existing target, the operation failed (again, correctly) because the device did not exist. However, the roll-back action associated with this second failure resulted in the target being removed. The roll-back action now checks whether the target pre-existed the failed actions, so the target is not removed in this circumstance.

BZ#677475

Attempting to run iscsid and the tgtd on the same machine results in semaphore errors being logged by both daemons because of an identifier collision. This has been corrected, and these errors no longer appear.

Enhancement

BZ#616402

Support for read-only target devices has been added to scsi-target-utils. Set read-only devices with the "--params" option of the tgtadm command, like so:

```
        tgtadm --lld iscsi --mode logicalunit --op update --tid 1 --lun
1
--params readonly=1
```

...or add "readonly 1" to the target element of your targets.conf file. Note that "allow-in-use" must also be set if you enable read-only targets in the targets.conf file.

All users of scsi-target-utils are advised to upgrade to this updated package, which resolves these issues.

1.260. seabios

1.260.1. RHBA-2011:0564 — seabios bug fix and enhancement update

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

This SeaBIOS package is a legacy BIOS implementation which can be used as a coreboot payload.

Bug Fixes

BZ#622350

When booting an MS-DOS 6.22 guest on an Intel host, SeaBIOS put the hardware in a state KVM couldn't handle, resulting in a crash. This patch restores segment limits in the handle_1589 code, so it no longer crashes.

BZ#643688

The ability to specify boot order from the qemu command line will allow for better control of a guest's behavior. Qemu should build list of all bootable devices and pass the preferred order into Seabios. This update applies 28 patches in order to do this. These include creating a separate IPL entry for each CD/DVD qemu in seabios, providing full EDD 3.0 information for virtio disk, adding the romfile_name() and strchr() functions, as well as functions for boot device path parsing. It tracks the source of each optionrom deployed, renames add_ordered_drive() to add_drive() and is used in map_hd_drive(), among many others. This will significantly enhance a user's experience and level of control.

BZ#666922

In order to support the above feature SeaBIOS needed to be rebased. Included in this patch are seven Red Hat Enterprise Linux 6 local patches that are forward ported: fix resume from S3 with QXL device; set Type 3 (chassis) manufacturer information to "Red Hat"; set system manufacturer/product name to Red Hat/KVM; set BIOS vender/version fields to Seabios/0.5.1; allow vendor/manufacturer/version product names to be set on config.h (*); do not advertise hpet to a guest OS; set CONFIG_S3_RESUME_VGA_INIT to 1.

BZ#673751

Previously, BIOS did not behave according to T13 EDD3.0 spec. This patch adds support for the spec, resulting in more information about interface and device paths. If a guest provides a buffer with enough space for T13 EDD information it will return EDD according to the T13 spec, otherwise it will use the Phoenix one.

BZ#671544

On a Windows virtual machine it was possible to 'Safely Remove' too many devices, including the graphics adapter, the PCI to ISA bridge device, and the PCI RAM controller, resulting in system instability. This patch uses the _RMV method to indicate whether device can be removed, thus fixing the issue.

BZ#668707

When guest was loaded to grub during reboot a "Guest moved using index from 0 to 580" error would occur, then the guest would quit. This update applies an upstream patch which sets vring_virtqueue to be zeroed, preventing old values being reused after reboot, fixing the problem.

BZ#663240

When running 'CHAOS-Concurrent Hardware And OS test', it passes while the child job 'run pwrtest' failed. This update applies a patch that turns RTC_S4 FACP bit to on, fixing the problem

All users of SeaBIOS are advised to upgrade to this updated package, which resolves these issues.

1.260.2. RHBA-2011:1346 — seabios bug fix update

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

The seabios package contains an open-source legacy BIOS implementation which can be used as a coreboot payload. It implements the standard BIOS calling interfaces that a typical x86 proprietary BIOS implements.

Bug Fix

BZ#740185

Previously, the smp_mtrr array was not large enough to hold all 31 entries of model-specific registers (MSRs) with current qemu-kvm implementations. As a consequence, installation of a Windows Server 2008 32-bit guest failed when more than one virtual CPU was allocated. With this update, the size of the smp_mtrr array has been increased to 32, and now Windows Server 2008 guests install successfully in the described scenario.

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

1.261. selinux-policy

1.261.1. RHBA-2011:0526 — selinux-policy bug fix and enhancement update

Updated selinux-policy packages that fix a number of bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#615731

Previously, an incorrect SELinux policy prevented the **wodim** CD and DVD authoring software from working correctly. This update corrects the SELinux policy, and **wodim** now works as expected.

BZ#630827

Due to an incorrect SELinux policy, attempting to use the guest operating system customization in **vCenter** failed. With this update, the relevant policy has been added, and SELinux no longer prevents users from customizing guest operating systems.

BZ#631523

When SELinux was enabled, suspending **VMware** virtual machines was either slowed down, or failed. With this update, the relevant SELinux policy has been corrected, and **VMware** virtual machines now suspend as expected.

BZ#631564

Previously, the **`allow_corosync_rw_tmpfs`** Boolean value allowed third party applications to create, write and read generic **`tmpfs`** (temporary file system) files. To prevent this undesired behavior, the Boolean value has been removed, and unless the unconfined policy is disabled, generic **`tmpfs`** files can now be managed using the **Corosync Cluster Engine**.

BZ#631952

When SELinux ran in enforcing mode, an incorrect SELinux policy prevented a custom **qemu-kvm** wrapper script, which is used to execute the **qemu-kvm** binary file, from running. With this update, the SELinux policy has been fixed so that the binary file can now be run as expected.

BZ#633959

Previously, the SELinux Multi-Level Security (MLS) policy prevented the **virsh dominfo** command from producing the expected results. This update fixes the relevant policy so that the command now works as expected.

BZ#634084

With SELinux running in enforcing mode, an attempt to run the **tgtd** service emitted Access Vector Cache (AVC) messages. With this update, the relevant policy rules have been modified to resolve this issue, and running the **tgtd** service no longer emits AVC messages.

BZ#634089

Due to an incorrect SELinux policy, running **cmirror** resulted in Access Vector Cache (AVC) messages. This bug has been fixed in this update so that **cmirror** now runs as expected.

BZ#634357

When a cluster was configured to use the **fence_scsi** I/O fencing agent, running either the **cman** startup script, or using the **fence_node -U [nodename]** command, resulted in failure. This update contains updated SELinux rules and adds the security file context for the **/var/lib/cluster/** directory, which allows a cluster with **fence_scsi** enabled to work properly.

BZ#634945

Due to an incorrect SELinux policy, the **smbcontrol** utility that sends messages to the **smbd**, **nmbd**, or **winbindd** service did not work properly. This bug has been fixed, the relevant policy has been added, and SELinux no longer prevents **smbcontrol** from working properly.

BZ#636683

When SELinux was enabled, users were unable to mount GFS2 file systems listed in the **/etc/fstab** file. With this update, SELinux rules have been added to allow the mount process to communicate with the **gfs_controld** service so that GFS2 file systems can now be mounted as expected.

BZ#637109

Previously, the SELinux security context was declared erroneously for the **/root/.ssh/** directory, which caused the **restorecon** command not to function properly. With this update, the relevant security context has been modified in order to fix this bug.

BZ#637135

The SELinux policy for the **rpc.quotad** service has been adjusted in order to make it work properly.

BZ#645658

Due to incorrect 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 the **unconfined_t** to **iptables_t** domain has been removed, and such commands now work as expected.

BZ#639074

With SELinux running in enforcing mode, resuming the operating system from suspend mode failed because of the **/etc/resolv.conf** file not having the correct security context. This was caused by **NetworkManager**, which ran under an incorrect SELinux domain (**devicekit_power_t**). With this update, the proper SELinux domain transition from **DeviceKit-power** to **NetworkManager** has been added, and resuming from suspend mode now works as expected.

BZ#639266

Due to incorrect SELinux policy rules, when a user tried to suspend or resume a laptop computer, Access Vector Cache (AVC) messages were displayed. This update fixes the relevant policy so that the suspend/resume actions no longer produce AVC messages.

BZ#639083

Previously, running the **passwd** command in single user mode failed when SELinux was enabled. With this update, the SELinux policy rules have been updated so that **passwd** can now access the system console as well as all terminals (TTYs) and pseudo-terminals (PTYs) on the operating system.

BZ#639230

Previously, the SELinux "xguest" user was trying to read login records. With this update, the SELinux policy rules have been updated, and the problem with the "xguest" user does not occur anymore.

BZ#639233

Previously, the SELinux "xguest" user was trying to read the **ConsoleKit** "history" log file. With this update, the SELinux rules have been updated so that the problem with the "xguest" user does not occur anymore.

BZ#640642

Due to incorrect SELinux policies, the **certmonger** service was not permitted to search through directories that contained certificates. This bug has been fixed by updating SELinux policy rules so that they now allow **certmonger** to access these directories.

BZ#644799

When a new user confined to SELinux was created and configured as the "staff_u" or "user_u" user, it was not possible to run the **ssh** command with a **ProxyCommand** option. With this update, the relevant SELinux policy has been corrected so that the **ssh** command with a **ProxyCommand** option works as expected.

BZ#646365

With this update, the SELinux security context for the **/etc/sysconfig/ip6tables.save** file has been corrected.

BZ#646856

Due to an incorrect SELinux policy, loading a kernel module that tried to create an entry in the **/sys/kernel/debug/** directory was not possible. This error has been fixed so that the updated SELinux policy rules now allow mounting of the **/sys/kernel/debug/** directory.

BZ#650136

The description of the **allow_httpd_mod_auth_ntlm_winbind** policy was fixed in this update.

BZ#651462

A new Pluggable Authentication Module (PAM) that replaces the **pam_tally2** module was added. The new module uses the **/var/run/faillock/** directory to store files that record recent login failures for individual users. Due to this change, a new SELinux security context was added for this directory.

BZ#655693

Due to incorrect SELinux policy rules, the **udevadm settle** command was very slow and took several minutes to complete. This update fixes the relevant policy so that the command now runs much faster.

BZ#657521

When the SELinux Multi-Level Security (MLS) policy was enabled, the **mount** command resulted Access Vector Cache (AVC) messages during the system startup. With this update, the relevant policy has been corrected and **mount** no longer produces AVC messages.

BZ#657568

Previously, the SELinux Multi-Level Security (MLS) policy prevented networking from starting successfully in **runlevel 1**. This update corrects the SELinux policy, and network can now be started as expected.

BZ#658410

When SELinux ran in enforcing mode, the **Cobbler** server did not work correctly. With this update, the SELinux policy has been fixed to permit requested accesses and **Cobbler** now works correctly.

BZ#658591

The **certmonger** service was not able to track 389-ds certificates due to an incorrect SELinux policy. This update corrects the SELinux policy so that **certmonger** is now able to track these certificates.

BZ#649432

When a user attempted to run the **slapi-nis** Network Information Service (NIS) server plug-in, Access Vector Cache (AVC) messages were displayed. This update fixes the relevant SELinux policy so that AVC messages do not appear anymore.

BZ#663054

Due to an incorrect SELinux policy, users confined to SELinux were not allowed to run the **ping** command if the **user_ping** Boolean value was enabled. With this update, the relevant policy has been corrected, and users confined to SELinux can run **ping** as expected.

BZ#663940

Previously, an Access Vector Cache (AVC) message could have been displayed when rebooting in single user mode with the SELinux Multi-Level Security (MLS) policy enabled. This update corrects the SELinux policy, and the AVC message no longer appears.

BZ#667071

Previously, the SELinux Multi-Level Security (MLS) policy prevented the **rpm -qa** command from producing the expected results. This update fixes the relevant policy so that the command works as expected.

Enhancements

BZ#655206

With this update, the number of packages in which the two SELinux policy modules used for the **389 Directory Server** were distributed has been reduced so that the modules are no longer distributed separately.

BZ#669439

To enable polyinstantiation with the SELinux Multi-Level Security (MLS), a new SELinux policy has been added for the **`namespace_init`** script.

BZ#682416

A new SELinux policy for the **`spice-vdagent`** command has been introduced in this update to enable the **`SPICE`** protocol features with SELinux.

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

1.261.2. RHBA-2011:1193 — selinux-policy bug fix update

Updated selinux-policy packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#719352

Prior to this update, the SELinux policy package did not allow the Red Hat Enterprise Virtualization agent to execute. This update adds the policy for Red Hat Enterprise Virtualization agents, so that they can be executed as expected.

BZ#727039

Previously, several labels were incorrect and rules for creating new 389-ds instances were missing. As a result, access vector caches (AVC) appeared when a new 389-ds instance was created through the 389-console. This update fixes the labels and adds the missing rules. Now, new 389-ds instances are created without further errors.

BZ#727078

Prior to this update, AVC error messages occurred in the audit.log file. With this update, the labels causing the error messages have been fixed, thus preventing this bug.

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

1.261.3. RHBA-2011:0935 — selinux-policy bug fix update

Updated selinux-policy packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#712410

Due to a constraint violation, the xinetd daemon was unable to connect to localhost in the enforcing mode, causing the operation to fail. With this update, the xinetd daemon is now trusted to write outbound packets regardless of the network's or node's MLS (Multi-Level Security) range, and the bug no longer occurs.

BZ#712194

Previously, a secadm SELinux user was not allowed to modify SELinux configuration files. With this update, the relevant SELinux policy has been fixed, and the secadm SELinux user can now modify these configuration files.

BZ#717688

Previously, the rsyslogd daemon was unable to send messages encrypted with the TLS (Transport Layer Security) protocol. This bug has been fixed, and rsyslogd now sends these encrypted messages as expected.

Users of selinux-policy are advised to upgrade to these updated packages, which fix these bugs.

1.262. setup

1.262.1. RHBA-2011:0524 — setup bug fix and enhancement update

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

The setup package contains a set of important system configuration and setup files, such as passwd, group, and profile.

Bug Fixes

BZ#616117

When logging in to an interactive login shell, the contents of the /etc/profile script are executed in order to set up an initial environment. Messages which should have been displayed to the user upon logging in to the Korn shell (ksh) were suppressed due to an internal test to determine whether the shell is a login shell that relied upon the value of the PS1 environment variable having already been set before /etc/profile was executed. However, this environment variable is set in the Korn shell only after /etc/profile is executed, which led to messages never being displayed to Korn shell users. This update provides an alternative test that does not rely on the PS1 variable being set before /etc/profile execution, with the result that messages are properly displayed to users of the Korn shell upon login.

BZ#620408

Bash provides the environment variable, PROMPT_COMMAND, containing a command that is called when a prompt is displayed. Previously, the PROMPT_COMMAND command used two separate echo commands. Consequently, if a background process returned text, the text might have displayed in the X terminal title rather than the terminal itself. In this updated package, the PROMPT_COMMAND command uses a single printf statement rather than two echo commands, ensuring returned text displays in the shell.

BZ#661645

Scripts in /etc/profile.d/ can contain special characters (eg spaces) in their filenames. Previously, if a script in the /etc/profile.d/ directory used a space in its filename, error messages were returned every time the shell was started. In this update, the script filenames in /etc/profile.d/ are formatted correctly

when called, and consequently, run as expected.

BZ#661681

Previously, using a user defined script in /etc/profile.d/ to modify umask settings failed when using an interactive login shell. Consequently, when this issue was encountered, the default umask settings were used. This updated package provides modified startup scripts, ensuring user defined scripts in /etc/profile.d/ set umask settings as instructed.

Enhancements

BZ#652287

The vdsm-reg package creates a user ID (UID) pair and group ID (GID) pair, both with the name "rhevm" and number "109". This user and group are used as a virtualization agent for Red Hat Enterprise Virtualization Manager. Previously, this UID/GID pair were not reserved during setup and other packages or administrators could accidentally assign those values to other users and groups. The setup package now reserves these UID and GID names and numbers. Accidental clashes with other users and groups are therefore avoided.

BZ#670231

The Automated Bug Reporting Tool (abrt) creates a user ID (UID) pair and group ID (GID) pair, both with the name "abrt" and number "173". The automated bug reporting process uses this user and group when it reports bugs. Previously, this UID/GID pair were not reserved during setup and other packages or administrators could accidentally assign those values to other users and groups. The setup package now reserves these UID and GID names and numbers for abrt. Accidental clashes with other users and groups are therefore avoided.

Users are advised to upgrade to this updated setup package, which resolves these issues and adds these enhancements.

1.263. shadow-utils

1.263.1. RHBA-2011:0790 — shadow-utils bug fix update

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

The shadow-utils package includes programs for converting UNIX password files to the shadow password format, as well as tools for managing user and group accounts.

Bug Fix

BZ#675168

Previously, the pam_tally.so module was used to write to /var/log/faillog. Since the module is no longer shipped, the faillog application that reads that file became obsolete. This update removes faillog from Red Hat Enterprise Linux 6.

All users of shadow-utils are advised to upgrade to this updated package, which fixes this bug.

1.264. smartmontools

1.264.1. RHBA-2011:0680 — smartmontools bug fix update

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

The smartmontools package contains two utility programs, smartctl and smartd, that enable the controlling and monitoring of Self-Monitoring, Analysis and Reporting Technology System (S.M.A.R.T.)-enabled storage systems. These utilities provide advanced warning of disk degradation and failure.

Bug Fixes

BZ#632423

The smartctl man page did not contain sufficient information about the CCISS (Compaq Smart Array) controller options. This man page section has been extended and provides more information and examples.

BZ#653434

In some cases, the smartmontools utilities passed to SCSI "ioctl" function certain values that the MegaRAID controller could not handle and S.M.A.R.T. self-tests on MegaRAID devices caused kernel errors and smartctl terminated unexpectedly. Such values are no longer passed to the MegaRAID controller and the bug is fixed.

All smartmontools users are advised to upgrade to this updated package, which resolves these issues.

1.265. sos

1.265.1. RHBA-2011:0773 — sos bug fix and enhancement update

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

The sos package contains a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

Bug Fixes

BZ#622528

Previously, the rhelVersion() function incorrectly identified the major release version in Red Hat Enterprise Linux 6. When the general.all_logs option of the general plug-in was enabled, some log files defined in the syslog.conf file were not retrieved and were missing in sos reports. This bug has been fixed and the rhelVersion() now always returns correct value of the Red Hat Enterprise Linux version.

BZ#622407

When the non-default lockdump feature was turned on, the cluster plug-in terminated with a traceback while sos was generating a report. This bug has been fixed, lockdump data are now present in reports and the cluster plug-in gives no error messages in the described scenario.

BZ#622527

Previously, reports generated by the sosreport utility did not include the /etc/anacrontab file, which may be essential for debugging cron issues. With this update, sos includes the /etc/anacrontab file in its reports.

BZ#622784

On IBM S/390 architecture, outputs from the parted and dumpe2fs utilities were not included in sos reports. This bug has been fixed and data retrieved from both utilities are now properly included in sos reports.

BZ#689387

When FIPS (Federal Information Processing Standard) compliance mode was active on the system, the sosreport program terminated with a traceback during generation of the MD5 checksum. As a consequence, no MD5 checksum was generated and no information about the name of the generated report was given, even though the report archive was generated correctly. This bug has been fixed, MD5 checksums are now generated in non-FIPS compliant mode (for compatibility with prior release) and SHA-2 checksums are generated in FIPS compliant mode.

BZ#691537

Previously, when sos was run without the rpm-python package installed, the sosreport program terminated with a traceback. With this update, the rpm-python package has been added into the sos spec file as a required package and this bug no longer occurs.

BZ#676522

Previously, sos did not back up files in the /etc/dhcp/ directory when it was run with the dhcp plug-in enabled and a DHCP server installed in the system. This bug has been fixed and sos now properly backs up these files in the described scenario.

BZ#659467

Due to a minor bug in the code, the startup plugin-in was unable to collect output from the chkconfig utility. This bug has been fixed and the chkconfig utility output is now properly included in sos reports.

Enhancements

BZ#675559

With this update, sos uses "dmsetup ls --tree" command output to print out summaries of complex device setups in sos reports. These summaries are much clearer to read compared to other options the dmsetup utility provides.

BZ#624162

With this update, sos includes the /etc/sssd/sssd.conf configuration file in its reports if the sssd package is installed and configured in the system.

BZ#678665

With this update, sos now supports next-generation X.509 entitlement certificates. These certificates are properly captured and included in sos reports.

BZ#679433

The lsblk utility shows the tree structure of all block devices in the system. With this update, sos captures the output of the lsblk utility and includes it in sos reports.

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

1.266. spice-client

1.266.1. RHBA-2011:1427 — spice-client bug fix update

An updated spice-client package that fixes a bug 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 access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

Bug Fix

BZ#725103

Although old SPICE-related packages (such as spice-cairo) are no longer required to be installed with the spice-client package, they were still needed by a previously installed spice-client or spice-server package. With the "Obsolete" lines in the package spec file, updating spice-client forced an update to spice-server as well, and vice versa. With this update, all "Obsolete" lines have been removed from the spice-client.spec file, thus fixing this bug.

All spice-client users that want to install spice-server on a client machine are advised to upgrade to this updated package, which fixes this bug, and uninstall the old SPICE-related packages when they are no longer needed.

1.267. spice-server

1.267.1. RHBA-2011:0705 — spice-server bug fix and enhancement update

An updated spice-server package that fixes several bugs and adds a number of enhancements is now available.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol designed for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

The spice-server package has been rebased to upstream version 0.8, which fixes the following bugs and adds the following enhancements (BZ#672035, BZ#645096):

Bug Fixes

BZ#674451

spice-server tried to use migration information even when it was not provided or required. This resulted in a segmentation fault in the client machine (the source of the migration operation). A check now determines whether the client has provided or is required to provide migration information.

BZ#670239

JPEG message encoding was handled differently between client and server, such that the server passed the client a value to determine an image's orientation, which the server interpreted as being invalid. This resulted in the client aborting. The value passed from the server is now the one the client expects, so the client no longer aborts.

BZ#622278

The palette cache was not always synchronized between client and server following live migration of a virtual machine with multiple monitors. The client side palette cache was not cleaned after migration, which caused the client to terminate unexpectedly. The target server now sends the "RESET" instruction to the client for all monitors, so this crash no longer occurs.

BZ#646483

A typographical error in qemu-kvm output has been corrected.

BZ#670245

Several superfluous dependencies were removed, including unnecessary dependencies on libcacard, CEGUI, X-libs and alsa packages.

BZ#674171

The spice-server and spice-client packages use common libraries in Red Hat Enterprise Linux 6.1. This renders the following packages obsolete: cairo-spice 1.8.7.2 and earlier, ffmpeg-spice 0.4.9-1 and earlier, pixman-spice 0.13.3-6 and earlier, and spice-common 0.4.2-8 and earlier. These removed and obsoleted packages are now recorded in the spice-server.spec file.

Note that if both spice-client and spice-server are installed on a system, upgrading one of them will also cause the other to be upgraded.

BZ#674937

Smart card (Common Access Card) support has been added to spice-server, allowing single sign-on and other card services such as signing and encryption.

All users requiring spice-server are advised to upgrade to this updated package, which adds these enhancements.

1.268. spice-xpi

1.268.1. RHBA-2011:0748 — spice-xpi bug fix update

An updated spice-xpi package that fixes three bugs is now available.

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. This package contains a SPICE extension that allows the client to be used from a web browser.

Bug Fixes

BZ#672761

Version was added to plugin name string. This allows the plugin version to be discovered from within the browser.

BZ#630601

Location and name of logfile & unix-domain-socket was changed, they are now placed in ~/.spicec/ and the name prefix is now spice-xpi.

BZ#672497

spicec is now searched for in /usr/bin, if not found in

Users planning to use the Red Hat Enterprise Virtualization Manager are advised to upgrade to this updated spice-xpi package.

1.269. squashfs-tools

1.269.1. RHBA-2011:0787 — squashfs-tools bug fix update

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

Squashfs is a highly compressed read-only filesystem for Linux. This package contains the utilities for manipulating squashfs file systems.

BZ#676774

A glibc update exposed a coding error in mksquashfs. This error resulted in dracut hanging while booting the Red Hat Enterprise Virtualization Hypervisor from PXE/CDROM/USB and an invalid LiveCD image being produced. The lines "memcpy(data_cache, data_cache + SQUASHFS_METADATA_SIZE," and "memcpy(directory_data_cache, directory_data_cache +" were changed respectively to "memmove(data_cache, data_cache + SQUASHFS_METADATA_SIZE," and "memmove(directory_data_cache, directory_data_cache +", thus a Red Hat Enterprise Virtualization Hypervisor boot from PXE/CDROM/USB now successfully completes without hanging during a boot.

BZ#655952

An error in unsquashfs code caused it to abort with "FATAL ERROR aborting: failed to read fragment table" during attempts to read a v3 image. The line "return;"is changed to "return TRUE;", thus unsquashfs is now able to read v3 images.

Users are advised to upgrade to this updated squashfs-tools package which resolves these issues.

1.270. squid

1.270.1. RHSA-2011:0545 — Low: squid security and bug fix update

An updated squid package that fixes one security issue and two bugs is now available for Red Hat Enterprise Linux 6.

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

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Security Fix

CVE-2010-3072

It was found that string comparison functions in Squid did not properly handle the comparisons of NULL and empty strings. A remote, trusted web client could use this flaw to cause the squid daemon to crash via a specially-crafted request.

Bug Fixes

BZ#666533

A small memory leak in Squid caused multiple "ctx: enter level" messages to be logged to "/var/log/squid/cache.log". This update resolves the memory leak.

BZ#639365

This erratum upgrades Squid to upstream version 3.1.10. This upgraded version supports the Google Instant service and introduces various code improvements.

Users of squid should upgrade to this updated package, which resolves these issues. After installing this update, the squid service will be restarted automatically.

1.270.2. RHSA-2011:1293 — Moderate: squid security update

An updated squid package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

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

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Security Fix

CVE-2011-3205

A buffer overflow flaw was found in the way Squid parsed replies from remote Gopher servers. A remote user allowed to send Gopher requests to a Squid proxy could possibly use this flaw to cause the squid child process to crash or execute arbitrary code with the privileges of the squid user, by making Squid perform a request to an attacker-controlled Gopher server.

Users of squid should upgrade to this updated package, which contains a backported patch to correct this issue. After installing this update, the squid service will be restarted automatically.

1.271. srptools

1.271.1. RHBA-2011:0755 — srptools bug fix and enhancement update

Updated srptools packages that fix several bugs and add various enhancements are now available.

In conjunction with the kernel ib_srp driver, srptools allows you to discover and use SCSI devices via the SCSI RDMA Protocol over InfiniBand.

Bug Fixes

BZ#591169

The srptools package did not include an init script to start the service automatically at system boot up. A new initscript has been added and can now be enabled to start automatically at each boot.

BZ#658633, BZ#658674

The srp_daemon does not reconnect to configured targets after several failure scenarios. The newly added initscript that starts the srp_daemon was written with this in mind and will restart the srp_daemon in the event one of these failure scenarios causes it to exit.

Users are advised to upgrade to this package, which resolves these issues and adds these enhancements.

1.272. sssd

1.272.1. RHSA-2011:0560 — Low: sssd security, bug fix, and enhancement update

Updated sssd packages that fix one security issue, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are linked to from the security descriptions below.

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

CVE-2010-4341

A flaw was found in the SSSD PAM responder that could allow a local attacker to crash SSSD via a carefully-crafted packet. With SSSD unresponsive, legitimate users could be denied the ability to log in to the system.

Bug Fixes

BZ#670259

The sssd package has been upgraded to upstream version 1.5.1, which provides a number of bug fixes and enhancements over the previous version.

BZ#582015

The Red Hat Enterprise Linux 6 Deployment Guide now contains a section on *Selecting an LDAP Schema*, which covers, among other things, the differences between the rfc2307 and the rfc2307bis LDAP schema.

BZ#598501

If SSSD was configured to use a non-anonymous bind (a bind DN (Distinguished Name) was specified and an authentication token, such as a password, was used), SSSD did not properly follow the LDAP referrals and only attempted to bind anonymously to the referred server. With this update,

non-anonymous bind on LDAP connections works as expected.

BZ#627165

The editing of the RPM configuration file during the installation of the sssd package caused a failure of the **rpmverify** check of the sssd package. With this update, the sssd package successfully passes the **rpmverify** check.

BZ#633406

Kerberos applications running on a secondary architecture of a **multilib** platform (for example, i686 on AMD64) were not 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#633487

Users would not always be assigned to all **initgroups** for which they were a member of 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#640602

SSSD did not correctly escape LDAP queries (for example, a username with the '\' character). As a result, an error was issued that caused SSSD to treat the LDAP server as unreachable. With this update, escaping of characters in LDAP queries has been fixed and works as expected.

BZ#645438

If a data provider died during an NSS (Network Security Services) request, the NSS responder died if the timeout of the open and unhandled requests was reached. This update introduces a reconnect handler which terminates the current request and does not cause the NSS responder to die.

BZ#645449

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#647816

The **gnome-screensaver** application could become unresponsive for more than two minutes when trying to unlock the screen with an incorrect password while SSSD was configured for proxy identification and authentication. This was due to faulty decrementing of in-progress authentication request child processes when they completed successfully. With this update, the process count is accurate, and the **gnome-screensaver** application no longer becomes unresponsive in the aforementioned case.

BZ#649286

SSSD has a cleanup task that removes unreferenced groups from the cache in order to keep the cache size down. However, only direct group memberships were checked by this cleanup task. Users who had a non-direct group as their primary group ID were not checked. As a result, it was possible for SSSD to purge legitimate groups from the cache. This could cause issues with group-based access control permissions such as **/etc/security/access.conf** and **/etc/sudoers**. With this update, groups, for which a user has the group as its primary GID, are no longer discarded from the cache.

BZ#651377

With this update, handling of expired accounts in the LDAP access provider has been improved. Additionally, the ***authorizedService*** LDAP attributes are now supported.

BZ#658158

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#659401

Previously, shutting down the **sssd** service (either by using the **service sssd stop** command, or with the **SIGTERM** signal) could cause SSSD to enter a busy-loop and never complete the shut down. This error has been fixed, and **sssd** no longer fails to shut down.

BZ#667059

Prior to this update, initial enumeration (which caches the entire set of available users and groups from the remote source to the local machine) failed after the **sssd** service was restarted when it was configured for a local domain. This was due to a ***tevent*** request that was not being posted properly. With this update, this issue has been fixed and enumeration works as expected.

BZ#667326

The **-s**/**--stdin** option of the **sss_obfuscate** command (which obfuscates a plain text password) reads the password to obfuscate from the standard input. However, not specifying the **-s**/**--stdin** option resulted in the same behavior. With this update, when no option is specified for the **sss_obfuscate** command, an interactive dialog for the password is shown.

BZ#667349

If TLS/SSL was used for identification, the LDAP provider would be terminated if an obfuscated password could not be decrypted (for example, if the plain text password was entered by accident). This was due to the LDAP provider failing to close the connection with the TLS/SSL server. With this update, an obfuscated password is decrypted at startup before any TLS/SSL operations.

BZ#670511

Configuring the system to allow a user to log into the system using **SFTP** (Secure File Transfer Protocol) only and be restricted to the user's home directory resulted in the **SFTP** connections being closed when SSSD was running on the system. This was due to improper closing of the file descriptors. This update adds additional checks which assure a correct closing of sockets and prevent the dropped SFTP connections.

BZ#670763

Not using enumeration and starting SSSD with a cleared cache caused the simple access provider to not be able to resolve the primary group at the time of authentication and resulted in an authentication failure due to faulty **initgroups** lookups. With this update, **initgroups** lookups have been improved and authentication no longer fails in the aforementioned case.

BZ#670804

Prior to this update, nested groups were not unrolled during the first enumeration causing

authentication of users in the nested group to fail. However, authentication did succeed after the second enumeration. With this update, unrolling of nested groups works as expected; authentication no longer fails.

BZ#671478

The configuration API files have been updated to reflect all current configuration options resolving errors where a configuration option specified in the **`/etc/sssd/sssd.conf`** file disappeared from the file after running **authconfig-tui** or **authconfig-gtk**.

BZ#674141

Traceback messages were displayed on the command line when executing the **`sss_obfuscate`** command as a non-root user. With this update, a human-readable error is displayed in such a case instead of the traceback messages.

BZ#674164

Prior to this update, the **`sss_obfuscate`** could fail if it could not establish (by reading the **`/etc/sssd/sssd.conf`** file) which domain was the default one. With this update, the **`sss_obfuscate`** command now always mandates the use of the **`-d`**/**`--domain`** option which requires a user to specify a domain to be used on the command line.

BZ#674172

Search filters for nested group lookups did not return correct results due to the **`rfc2307bis_nested_groups_update_sysdb()`** and **`save_rfc2307bis_user_memberships()`** functions calling the **`sysdb_search_groups()`** function with a non-sanitized ***`member_dn`*** parameter. With this update, search filters have been fixed and work as expected.

BZ#674515

The **`-p`**/**`--password`** option of the **`sss_obfuscate`** command was not properly setting the provided password (specifically, it always used an empty string instead of the provided password). As a result, SSSD was unable to successfully complete an LDAP bind. This update removes the **`-p`**/**`--password`** option of the **`sss_obfuscate`** command as it is not safe to pass a password on the command line.

BZ#675284

Prior to this update, when SSSD was configured to require the **`authorizedService`** attribute for access control, even though a user's authentication request completed successfully, the following message was logged in the **`/var/log/secure`** log file:

```
Authorized service attribute has no matching rule, access denied
```

This update fixes this faulty behavior and no error messages are logged on successful authentication requests.

BZ#676401

Originally supported time rules in the HBAC (Host-Based Access Control) rules in FreeIPAv2 have been dropped from the final version. However, SSSD expected these rules to be functional and caused unexpected denials if they were not. With this update, time rules have been removed from SSSD and no longer cause denial errors.

BZ#676911

Prior to this update, SSSD always attempted to use the **START_TLS** function when performing LDAP authentication. However, some LDAP servers (especially those configured to work behind SSL accelerators) cannot handle TLS (Transport Layer Security) over LDAPS (Secure LDAP) which prevented authentication from succeeding on those platforms. With this update, SSSD no longer attempts to start TLS if it is connected over LDAPS.

BZ#677318

A check for a renewable TGTs (Ticket Granting Ticket) at startup did not work properly because the **ccache** file was not being checked. With this update, the **ccache** file is checked for any renewable TGTs at every startup unless indicated otherwise.

BZ#677588

SSSD could crash when renewing TGTs because some of the TGTs were not being removed from the renewal list after they already have been successfully renewed. With this update, a TGT is properly removed from the renewal list after being successfully renewed.

BZ#678091

Due to SSSD originally having its HBAC support designed around an early preview of FreeIPAv2, SSSD expected that HBAC rules would be stored in the ***cn=account*** subtree of FreeIPAv2. However, the final version of FreeIPAv2 stores them in the ***cn=hbac*** subtree instead. This resulted in denial errors from SSSD because no rules could be accepted. With this update, denials/permissions are based on the HBAC rules, and SSSD no longer returns denial errors.

BZ#678410

Modifying or deleting a user/group account on an LDAP server did not result in an update of the cache on a login attempt. With this update, the cache is always properly updated during the login process. Outside of a login attempt, entries remain as they were cached until the cache timeout expires.

BZ#678593

At any PAM (Pluggable Authentication Modules) action occurring online, SSSD is supposed to perform an **initgroups()** request to the backend to ensure that user and group memberships are accurate for the login. However, a bug has been discovered which causes this lookup to be performed on the first domain in the list of domains only. This update fixes this issue; **initgroups()** requests are properly processed on all existing domains.

BZ#678614

The netgroup search base in SSSD has been updated to match the one specified in FreeIPAv2.

BZ#678777

When performing an **initgroups()** request on a user, the IPA provider did not properly remove group memberships from the local cache when they were removed from the IPA server. With this update, a removed group is no longer present in the local cache.

BZ#679082

This update ensures that if the **ipa-client-install** command (which configures an IPA client) is executed with the **--realm** option, the specified realm is set in all SSSD configuration files in both the **realm** and the **krb5_realm** configuration directives.

BZ#680367

Prior to this update, SSSD was not thread safe for certain calls. This update adds additional mutual exclusion algorithms around nss operations and serializes them. pam functions, which only use the provided pam handler, now have protected socket operations. As a result, SSSD is now thread safe.

BZ#680440

Prior to this update, SSSD did not properly handle a change of a Kerberos server's IP address.

BZ#680442

Specifying a single server name in the **`ipa_server`** option in the **`/etc/sssd/sssd.conf`** file resulted in a successful dynamic update of the DNS records of the IPA DNS server. However, if two or more servers are specified, the update failed. This update addresses this issue, and specifying multiple servers in the **`ipa_server`** works as expected.

BZ#680932

If the RFC2307bis schema was used and the server did not have the ***`memberOf`*** attributes defined, SSSD attempted to remove them from the **`sysdb`** cache. However, this attribute is exclusively managed by the **memberOf** plugin. With this update, SSSD no longer attempts to delete the ***`memberOf`*** attribute under any circumstances.

BZ#682340

Attempting to stop the IPA services via the **`ipactl`** (an IPA server control interface) command as a non-root user resulted in a segmentation fault. With this update, a segmentation fault no longer occurs.

BZ#682807

If a requested netgroup does not exist, SSSD adds the name to the negative cache. If the end of the lifetime for the cache entry was reached, the **`sssd_nss`** module tried to delete the entry and failed with a segmentation fault. With this update, the aforementioned netgroups are properly handled, and a segmentation fault no longer occurs.

BZ#682850

With this update, both SSSD and IPA use the Kerberos realm as the base domain name.

BZ#683158

In certain cases, SSSD failed when it encountered a non-POSIX compliant group (contained no GID attribute). With this update, non-POSIX-compliant groups are ignored and no longer cause SSSD to fail.

BZ#683255

If SSSD failed to parse a broken netgroup entry from the LDAP server, a new request for the same group timed out and returned only after the client timeout of 5 minutes was exceeded. With this update, the state of a netgroup's hash entry is changed if a netgroup cannot be parsed.

BZ#683431

Using LDAP as an identity provider and Kerberos as the authentication provider and setting the Kerberos provider backend offline could result in an improper termination of the connection with LDAP. As a result, SSSD started to consume 100% of the CPU and logged error messages into the SSSD log. With this update, an LDAP connection is properly released and no longer causes the aforementioned issues.

BZ#683860

SSSD failed when it encountered nested group memberships with non-POSIX-compliant groups in the middle of the nest. With this update, non-POSIX-compliant groups are ignored and no longer cause SSSD to fail.

BZ#683885

The LDAP RFC2307 schema, while not explicitly allowing it, did not forbid the use of a multi-valued attribute for the name of a group. Previously, SSSD returned an error and aborted an **`initgroups()`** call if it attempted to process a such a group. With this update, groups with multi-values attributes are skipped when issuing an **`initgroups()`** call.

BZ#688491

Specifying Kerberos as the access control provider in the **`/etc/sssd/sssd.conf`** file (**`access_provider = krb5`**) resulted in a traceback error when trying to update all SSSD-related files with the **`authconfig --enablesssd --enablesssdauth --updateall`** command. With this update, this issue has been fixed; all SSSD-related files are updated and SSSD starts as expected.

BZ#689886

Performing an **`initgroups()`** call in the IPA provider caused only the user the call was being issued on to be stored in the cache. This was because the group, the user was a part of, only contained that user in the cache and was not being refreshed with the rest of the users of that group. Thus, a command such as **`getgrnam`** would only show the single user of that group. With this update, all users are properly taken into account in the aforementioned case.

BZ#690131

A traceback error is no longer returned when terminating the **`sss_obfuscate`** command with the **`CTRL`**+**`D`** shortcut.

BZ#690421

Under certain circumstances, if nested groups were not processed successfully due to a misconfiguration on an RFC2307bis LDAP server, a segmentation fault occurred. With this update, an appropriate error message is returned instead of a segmentation fault in the aforementioned case.

BZ#690866

Groups which have a zero-length string specified in the ***`memberuid`*** attribute are now properly handled, and no longer cause new lookups to not be cached properly.

BZ#691678

SSSD now correctly falls back to the ***`cn`*** attribute for **`GECOS`** information (entry in the **`/etc/passwd`** file) if the **`GECOS`** field is empty, making SSSD fully compliant with section 5.3 of RFC 2307.

BZ#694146

For large cache files, if a user was removed from a group in LDAP, memory allocation could grow exponentially while processing the removal from the cache, potentially resulting in an OOM (Out of Memory) situation. With this update, this issue has been fixed, and SSSD no longer allocates unnecessarily large amounts of memory when removing a user from a group in LDAP.

BZ#694444

Prior to this update, the SRV records result processing code attempted to filter out duplicate entries, but failed to do so properly. This update removes the detection of duplicates from SRV result processing, resolving this issue.

BZ#694783

If there was no rootDSE (the root of the directory data tree on a directory server) data present, the LDAP provider crashed. This update includes various fixes that resolve this issue.

BZ#701700

The **`select()`** call could only handle file descriptors smaller than 1024. If an **`sssd`**, **`nss`**, or **`pam`** client was called from an application with many open files, the file descriptor used by the client could be larger than 1024, which resulted in undefined and unexpected behavior. With this update, the **`poll()`** call is used instead of the **`select()`** call, eliminating any possible memory corruption issues in the calling process.

Enhancements

BZ#660323

If service discovery is used in a domain back end, the DNS domain used for the search can now be specified by the new **`dns_discovery_domain`** option. If not specified, the domain part of the machine's hostname is used (previously, it was the name of the SSSD configuration domain). As a backwards-compatibility measure, the SSSD domain is used in case the domain part cannot be acquired from the machine's hostname.

BZ#442680

SSSD now supports automatic Kerberos ticket renewal which provides Kerberos tickets for long-running processes or cron jobs even when a user logs out.

BZ#614535

Support for obfuscated (non-plain text) passwords in the SSSD configuration files has been added.

BZ#652759

SSSD now provides support for account lockout policies when using Active Directory or IPA. Additionally, SSSD provides support for shadow access control when using LDAP.

Users of SSSD should upgrade to these updated packages, which contain backported patches to correct this issue, fix these bugs, and adds these enhancements.

1.272.2. RHBA-2011:1143 — sssd bug fix update

Updated sssd packages that resolve an issue 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 back-end system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects such as FreeIPA.

Bug Fix

BZ#727041

Previously, SSSD did not properly close its PAM sockets after an authentication attempt, which eventually resulted in process resource exhaustion and a denial of service situation. The code has been modified to fix this issue, and file descriptors are now properly released when they are no longer in use.

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

1.272.3. RHBA-2011:0925 — sssd bug fix update

Updated sssd packages that fix two 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 (Name Service Switch) and PAM (Pluggable Authentication Modules) interface toward the system and a pluggable back-end system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects such as FreeIPA.

Bug Fixes

BZ#716905

Previously, SSSD relied on the inotify kernel subsystem to detect whether a DNS resolver file had been changed. If inotify returned an error (for example due to resource exhaustion), SSSD terminated unexpectedly and network logins no longer worked. With this update, SSSD itself detects the failure in the described scenario and falls back to the five-second polling, fixing this bug.

BZ#716909

When SSSD communicated with an OpenLDAP server, which supported server-side password policies but did not list them in the "supportedControl" attribute of the server's rootDSE entry, SSSD terminated unexpectedly with a segmentation fault. This was a regression introduced in version 1.5.1-34.el6 of the sssd package. An upstream patch has been provided to fix this bug.

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

1.272.4. RHBA-2011:0849 — sssd bug fix update

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

SSSD provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides NSS (Name Service Switch) and PAM (Pluggable Authentication Modules) interfaces toward the system and a pluggable back end system to connect to multiple different account sources.

Bug Fixes

BZ#708352

When the first DNS entry defined in the /etc/resolv.conf file was unreachable, the sssd utility failed to try to connect to any subsequent DNS server to resolve the SRV record. This caused sssd to permanently operate in offline mode. This bug has been fixed and sssd is now able to connect to an alternate server if the primary server is down.

BZ#708353

The sssd client terminated when the ldap_default_authtok_type option was not configured. With this update, the ldap_default_authtok_type option now defaults to "password" if it is not specified in the /etc/sssd/sssd.conf file and the bug no longer occurs.

Users of sssd are advised to upgrade to these updated sssd packages, which fix these bugs.

1.273. strace

1.273.1. RHBA-2011:0338 — strace bug fix update

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

The strace program intercepts and records the system calls called and received by a running process. It can print a record of each system call, its arguments and its return value.

Bug Fixes

BZ#533199

Previously, the manual pages and the output of "strace --help" contained inconsistencies. This update corrects these errors. Now, the descriptions for the listed options on the manual pages and in the output of ‘strace --help’ contain the same information.

BZ#642389

Previously, the CLONE_PTRACE flag was set in the arguments of a clone when it was called with the flag CLONE_UNTRACED. Due to this behavior, strace traced the child process for clones called with the flag CLONE_UNTRACED.This update does no longer trace children with CLONE_UNTRACED. Now, the tracing of child processes behaves as expected.

BZ#654515

Previously, the decoding of 64-bit arguments of certain system calls was incorrect. This update corrects this issue. Now, 64-bit arguments of system calls are decoded as expected.

BZ#661748

Previously, waitpid waited for children created by clone even when the options "__WCLONE" or "__WALL" were not present. Due to this behavior, the process became suspended. This update does no longer suspend the process in the waitpid system call.

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

1.274. subscription-manager

1.274.1. RHBA-2011:0902 — subscription-manager bug fix update

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

The Subscription Manager tool allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

Warning: Before applying this update, there is a manual step that you may need to perform. This step

assumes that you are using the new subscription manager entitlement tooling to apply software updates. If you are encountering an "[Errno 14] problem with the local client certificate" error message when executing yum commands, you will need to run the following commands as root:

```
    # rm -f /etc/pki/entitlement/*
# subscription-manager refresh
```

Note that systems that are using Red Hat Network Classic for software entitlement updates do not need to perform this manual step before applying this errata update.

Bug Fixes

BZ#712409

When the subscription-manager utility had been upgraded, it put incorrect data to the sslclientkey repository parameter value. Consequently, when the yum utility was executed to install a software, yum terminated with the "[Errno 14] problem with the local client certificate" error message. The bug in subscription-manager has been fixed and yum can now be run without any certificate errors.

BZ#712128

Previously, running the firstboot utility with the "-r" option, while the subscription-manager-firstboot utility was already installed, caused firstboot to terminate with a traceback; firstboot also failed to display a message stating that the computer was already registered with Red Hat Network. This bug has been fixed, firstboot now displays the warning message properly and no tracebacks are issued in the described scenario.

BZ#712130

Two variations were used in the ProductName parameter for the workstation subscription: "Red Hat Enterprise Linux Workstation" and "Red Hat Enterprise Linux 6 Workstation". As a consequence, users running the "subscription-manager list --installed" command, while subscribed to the "Red Hat Enterprise Linux Workstation" subscription, got a misleading report. With this update, the ProductId parameter is used instead to compare subscriptions in the described scenario, and the bug no longer occurs.

BZ#712408

Previously, the "Start Date" and "End Date" fields in the Contract Selection dialog window of the subscription-manager-gui utility were not populated. With this update, the dates are displayed as expected.

All users of subscription-manager are advised to upgrade to these updated packages, which fix these bugs.

1.274.2. RHBA-2011:0822 — subscription-manager bug fix update

Updated subscription-manager packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The Subscription Manager tool allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

Bug Fixes

BZ#702029

Prior to this update, the graphical user interface of the Subscription Manager utility incorrectly listed unlimited subscriptions as "-1". This update adapts the Subscription Manager to mark such subscriptions as "unlimited".

BZ#702030

Due to incorrect handling of user's locale settings, the "My Subscriptions" tab in the previous version of the Subscription Manager may have displayed incorrect end dates. With this update, the underlying source code has been adapted to address this issue, and the "My Subscriptions" tab now displays correct end dates.

BZ#702398

Previously,the Subscription Manager used the same key.pem file for all entitlements. However, the NSS (Network Security Services) libraries require a different file for each entitlement, and an attempt to install packages on a system with more than one subscription therefore failed with an error message similar to the following:

```
        [Errno 14] PYCURL ERROR 22 - "NSS: private key not found for
certificate: PEM Token #1:1310636811763322869.pem"
```

This update adapts the Subscription Manager to create a unique key.pem file for each entitlement, so that packages can now be installed as expected on such systems.

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

1.275. subversion

1.275.1. RHSA-2011:0862 — Moderate: subversion security update

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

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

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.

Security Fixes

CVE-2011-1783

An infinite loop flaw was found in the way the mod_dav_svn module processed certain data sets. If the SVNPathAuthz directive was set to "short_circuit", and path-based access control for files and directories was enabled, a malicious, remote user could use this flaw to cause the httpd process serving the request to consume an excessive amount of system memory.

CVE-2011-1752

A NULL pointer dereference flaw was found in the way the mod_dav_svn module processed requests submitted against the URL of a baselined resource. A malicious, remote user could use this flaw to cause the httpd process serving the request to crash.

CVE-2011-1921

An information disclosure flaw was found in the way the mod_dav_svn module processed certain URLs when path-based access control for files and directories was enabled. A malicious, remote user could possibly use this flaw to access certain files in a repository that would otherwise not be accessible to them. Note: This vulnerability cannot be triggered if the SVNPathAuthz directive is set to "short_circuit".

Red Hat would like to thank the Apache Subversion project for reporting these issues. Upstream acknowledges Joe Schaefer of the Apache Software Foundation as the original reporter of CVE-2011-1752; Ivan Zhakov of VisualSVN as the original reporter of CVE-2011-1783; and Kamesh Jayachandran of CollabNet, Inc. as the original reporter of CVE-2011-1921.

All Subversion users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, you must restart the httpd daemon, if you are using mod_dav_svn, for the update to take effect.

1.276. sudo

1.276.1. RHSA-2011:0599 — Low: sudo security and bug fix update

An updated sudo package that fixes one security issue and several bugs is now available for Red Hat Enterprise Linux 6.

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

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root.

Security Fix

CVE-2011-0010

A flaw was found in the sudo password checking logic. In configurations where the sudoers settings allowed a user to run a command using sudo with only the group ID changed, sudo failed to prompt for the user's password before running the specified command with the elevated group privileges.

Bug Fixes

BZ#603823

When the "/etc/sudoers" file contained entries with multiple hosts, running the "sudo -l" command incorrectly reported that a certain user does not have permissions to use sudo on the system. With this update, running the "sudo -l" command now produces the correct output.

BZ#634159

Prior to this update, the manual page for sudoers.ldap was not installed, even though it contains important information on how to set up an LDAP (Lightweight Directory Access Protocol) sudoers source, and other documents refer to it. With this update, the manual page is now properly included in the package. Additionally, various POD files have been removed from the package, as they are required for build purposes only.

BZ#652726

The previous version of sudo did not use the same location for the LDAP configuration files as the nss_ldap package. This has been fixed and sudo now looks for these files in the same location as the nss_ldap package.

BZ#665131

When a file was edited using the "sudo -e file" or the "sudoedit file" command, the editor being executed for this task was logged only as "sudoedit". With this update, the full path to the executable being used as an editor is now logged (instead of "sudoedit").

BZ#688640

A comment regarding the "visiblepw" option of the "Defaults" directive has been added to the default "/etc/sudoers" file to clarify its usage.

BZ#615087

This erratum upgrades sudo to upstream version 1.7.4p5, which provides a number of bug fixes and enhancements over the previous version.

All users of sudo are advised to upgrade to this updated package, which resolves these issues.

1.276.2. RHBA-2012:0513 — sudo bug fix update

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

The sudo (super user do) utility allows system administrators to give certain users the ability to run commands as root.

Bug Fix

BZ#802439

A race condition in the signal handling code caused the sudo process to become unresponsive after receiving the SIGCHLD signal. This update modifies the signal handling to prevent the race condition, which ensures that the sudo process no longer hangs under these circumstances.

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

1.277. syslinux

1.277.1. RHBA-2011:0634 — syslinux bug fix update

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

The syslinux utility is responsible for booting the operating system kernel.

Bug Fix

BZ#622346

The machine will hang when using syslinux 3.86 to download vmlinuz and initrd with the Broadcom BCM5723 Ethernet chip.

Users of syslinux are advised to upgrade to this updated package, which resolves this issue.

1.278. sysstat

1.278.1. RHBA-2011:0668 — sysstat bug fix and enhancement update

An updated sysstat package that fixes various bugs and adds two enhancements 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 Fixes

BZ#595231, BZ#536928

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.

BZ#637705

on a system with a running KVM virtual machine and under very special circumstances, the sar utility may have produced an output that contained incorrect values. This error no longer occurs, and the sar utility now always produces the correct output.

BZ#624130

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#690402

previously, the "iostat -n" command was not aware of any NFS shares that were mounted or unmounted while processing. Consequently, iostat reported incorrect values such as:

nfs:/share 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00

In this updated package the "iostat -n" command is made aware of any NFS shares that are mounted or unmounted while the command is running, and reports meaningful results.

BZ#631841

under certain circumstances, the sar tool was unable to accurately report system activity on systems with multiple CPUs that also use the tickless kernel. If this issue was encountered, sar would report values of 0.00 for all values of some CPUs. In this updated package, sar correctly handles the behavior of the tickless kernel and returns accurate results.

Enhancements

BZ#592283

previously, iostat lacked the ability to provide granular I/O statistics for Common Internet File System (CIFS) shares. This updated iostat package includes the new cifsiostat tool, providing the ability to generate I/O statistics for CIFS shares.

BZ#690400

previously, default parameters could not be set for the sadc command. In this updated package, parameters for the "sadc" command can be set using the "${SADC_OPTIONS}" variable located in the "/etc/sysconfig/sysstat" configuration file

All users of sysstat are advised to upgrade to this updated package which fixes these bugs and adds these enhancements.

1.279. system-config-firewall

1.279.1. RHSA-2011:0953 — Moderate: system-config-firewall security update

Updated system-config-firewall 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.

system-config-firewall is a graphical user interface for basic firewall setup.

Security Fix

CVE-2011-2520

It was found that system-config-firewall used the Python pickle module in an insecure way when sending data (via D-Bus) to the privileged back-end mechanism. A local user authorized to configure firewall rules using system-config-firewall could use this flaw to execute arbitrary code with root privileges, by sending a specially-crafted serialized object.

Red Hat would like to thank Marco Slaviero of SensePost for reporting this issue.

This erratum updates system-config-firewall to use JSON (JavaScript Object Notation) for data exchange, instead of pickle. Therefore, an updated version of system-config-printer that uses this new communication data format is also provided in this erratum.

Users of system-config-firewall are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. Running instances of system-config-firewall must be restarted before the utility will be able to communicate with its updated back-end.

1.280. system-config-kickstart

1.280.1. RHBA-2011:0167 — system-config-kickstart bug fix update

An updated system-config-kickstart package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The system-config-kickstart package contains Kickstart Configurator, a graphical tool for creating kickstart files.

Bug Fixes

BZ#610740

When a user opened an existing file, Kickstart Configurator did not clear the partition information, and

the configuration from the file was incorrectly added to the previous configuration. With this update, the underlying source code has been adapted to address this issue, and opening a file now clears the previous partition information as expected.

BZ#633202

In the "Authentication" tab, the default hash function for shadow passwords was set to MD5. This update changes the default option to SHA-512.

Users of system-config-kickstart are advised to upgrade to this updated package, which resolves these issues.

1.281. system-config-users

1.281.1. RHBA-2011:0730 — system-config-users bug fix and enhancement update

An updated system-config-users package that fixes several bugs and adds one enhancement are now available for Red Hat Enterprise Linux 6.

The system-config-users utility provides a graphical interface for adding and removing users and groups to the system. Once started, system-config-users provides a help feature to assist in learning the interface.

Bug Fixes

BZ#582205

Previously, passwords deemed too simple were always prohibited. This update only warns about passwords that are deemed unsuitable or too weak. Now, also short passwords are accepted.

BZ#599214

Previously, system-config-users did not always detect if a home directory could be created correctly before actually doing it. Due to this problem, system-config-users did not create a home directory on certain file systems (e.g. home directories located beneath an autofs mount-point) but acted on the assumption that it did. As a workaround, this update tries to create the home directory before creating the user in system-config-users.

BZ#628730

Previously, system-config-users failed to start if the maximum allowable length for user or group IDs (UID/GID) was already allocated. This update handles this situation by ignoring such high UIDs/GIDs where it needs to automatically allocate user or group IDs.

BZ#612172

Previously, a search for users and groups would only search for names beginning with the search string. Due to this behavior, names that had the string somewhere else in the name were ignored. This update searches for substrings in user and group names.

BZ#629469

Previously, several on-screen messages were not correctly translated in some languages. This update corrects the translated strings. Now, all messages are correctly translated.

Enhancement

BZ#571571

Previously, users could not force password expiration from the graphical user interface. This update allows for forced expiry of passwords without the need to use command line utilities.

All users of the system-config-users utility are advised to upgrade to this updated package, which fix these bugs and adds this enhancement.

1.282. systemtap

1.282.1. RHSA-2011:0842 — Moderate: systemtap security update

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

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

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.

Security Fixes

CVE-2011-1769, CVE-2011-1781

Two divide-by-zero flaws were found in the way SystemTap handled malformed debugging information in DWARF format. When SystemTap unprivileged mode was enabled, an unprivileged user in the stapusr group could use these flaws to crash the system. Additionally, a privileged user (root, or a member of the stapdev group) could trigger these flaws when tricked into instrumenting a specially-crafted ELF binary, even when unprivileged mode was not enabled.

SystemTap users should upgrade to these updated packages, which contain a backported patch to correct these issues.

1.282.2. RHSA-2011:1088 — Moderate: systemtap security update

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

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

SystemTap is an instrumentation system for systems running the Linux kernel. The system allows developers to write scripts to collect data on the operation of the system.

Security Fixes

CVE-2011-2502

It was found that SystemTap did not perform proper module path sanity checking if a user specified a custom path to the uprobes module, used when performing user-space probing ("staprun -u"). A local user who is a member of the stapusr group could use this flaw to bypass intended module-loading restrictions, allowing them to escalate their privileges by loading an arbitrary, unsigned module.

CVE-2011-2503

A race condition flaw was found in the way the staprun utility performed module loading. A local user who is a member of the stapusr group could use this flaw to modify a signed module while it is being loaded, allowing them to escalate their privileges.

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

1.282.3. RHBA-2011:0651 — systemtap bug fix and enhancement update

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.

With this update SystemTap is now re-based on upstream version 1.4. This re-base features several enhancements.

Bug Fixes

BZ#600382

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.

BZ#609636

Unwinding through a Common Flash Memory Interface (CFI) from the **.debug_frame** section in a prelinked shared library was broken on an i686. This update ensures user space shared libraries are no longer a special case, but are treated similarly to other sections using .debug_frames for unwinding, resulting in unwinding working as expected on an i686. This also fixes a similar issue with unwinding through kernel modules.

BZ#618867

Probing ioblock.stp failed with the error "ERROR: kernel read fault" before shutting down. This was due to an error with the null pointer dereference. In this update, before kread to occur, a check is added to monitor another parameter in the "bio" structure. This gives the count of the vector pages allocated. If there are none the pointer is not dereferenced. This allows ioblock.stp to be probed as expected.

BZ#624657

When sending stapio a signal to unload a module, it would fail with an error saying that the script was still running. This was because, after the signal was sent, it was not waiting for the module to be unloaded before continuing with the script. This update adds a check to ensure the module has finished being unloaded before declaring a success, allowing the module to be unmounted as expected.

BZ#625849

SystemTap provides bench.sh, a script that compiles benchmark code on a system, then monitors the system as it runs the code. The benchmark code previously provided with SystemTap was designed to run on the 64-bit x86 architecture. Therefore, attempting to run the script on other architectures would fail. This updated package provides code that runs on architectures other than 64-bit x86. Users of SystemTap can now measure probe performance on all architectures supported by Red Hat.

BZ#634995

This update rebases SystemTap from the upstream release which includes several new features, including the **`--remote`** command, allowing users to build the SystemTap module locally, and execute remotely via SSH.

BZ#640097

An automated stress test for userspace apps with extensive probing failed with segmentation faults. This was caused by two things. The first was uprobes with vfork were not being handled correctly. Now, when a vfork'ed thread executes, probes are not removed from the vfork parent while the thread associations are cleaned up. The second problem was regarding uprobes problems with empty functions/newer GCCs. With this patch, the newer GCCs that were emitting conditional returns for empty functions, which uprobes instruction handler was not expecting, have been fixed. This allows the probing to proceed as expected.

BZ#643866

When testing the client.stp script, libvirtd printed out a lot of errors when it started up. This occurred whenever the CLONE_NEWPID flag was called as SystemTap was looking for the Process Identifier (PID) in the private PID namespace instead of the public PID namespace. This has been rectified in this patch, allowing the client.stp script to run as expected.

BZ#607227

Previously, the code for starting, stopping, and restarting SystemTap was defined in SystemTap's own initscript rather than using the globally defined behaviors on the system. SystemTap's own handling of the 'restart' action did not start SystemTap if it was not already running. This updated package copies the $SCRIPTS global scripts as a basis for its initscript actions. The 'restart' action therefore has the same default behavior as other initscripts on the system and additionally now honors the 'force-reload', 'reload', 'condrestart' and 'try-restart' actions.

BZ#646871

After a prelink was used, attempting to use SystemTap user-space probes that target functions or statements in certain shared libraries, or exectuables based on separate debuginfo, resolved to the wrong PC location in a prelinked binary. This resulted in the intended probes failing to fire at the correct place in the program, leading to the program crashing or misbehaving due to a corrupted instruction sequence resulting from incorrect breakpoint insertion. This update adjusts the libdwfl (libdw.so) library code to use more reliable methods of compensating for prelink's effect on the address layout of a binary while aligning a runtime PC address with an address computed from the separate debuginfo file. This allows SystemTap probes to work the same on prelinked binaries as they do on the same binaries when they have not been adjusted by prelink.

BZ#670644

When attempting to build an exectuable of Ruby including SystemTap marker, some arguments for markers were truncated to 8 bits in size. This was caused by the function "%rbx being an 8 bit register rather than the full 64 bit register. This function has been changed to 64 bit which resolves the issue.

BZ#671004

GCC sometimes emitted the code sequence **`repnz;ret`** to end a function. SystemTap's uprobes module then rejected this as an unknown instruction sequence. This patch allows such instructions to be treated as **`rep;ret = ret`**, allowing stap to run without risk, even with such optimized GCC code.

BZ#676641

Previously **`/user/bin/dtrace`** was provided by **`systemtap-sdt-devel`**, while dtrace(1) man page was provided by SystemTap. This caused confusion when the binary was not found. This update puts the dtrace(1) man page in the same package as the binary, removing the confusion and resolving this issue.

BZ#681190

Previously, SystemTap's user module build id check was not aware of address space. Consequently, running a user space tracing script could fail. In this updated package, the get_user() function in the build id check is bracketed by set_fs(), which ensures that the function is called in the correct space and that user space tracing scripts run correctly.

BZ#683569

The SystemTap Beginner's Guide gave inaccurate instructions on how to configure yum to access the debuginfo packages. With Red Hat Enterprise Linux 6, the debuginfo packages are located in the Red Hat Network. With this patch the documentation now reflects this.

BZ#690597

Previously, python's **`sys/sdt.h`** probes were not being activated on IBM System z architectures. This was because some IBM System z architectures do not have noexec mappings for data sections so the .probes section with SDT semaphores was mapped with RWX rather than RW-. This patch checks VM flag needs to accommodate this giving the ability to deal with mappings that are both executable and writable so semaphores can be found.

BZ#691693

The testcase **`systemtap.base/bench.exp`** FAILed. This was due to a change of output from Red Hat Enterprise Linux 6.0 and Red Hat Enterprise Linux 6.1. This patch updates the test to handle newer probe timing report output, preventing this.

BZ#691750

The testcase **`systemtap.printf/ring_buffer.exp`** had 1 FAIL. This was because the variable was already static so needed to be initialized to 0. This patch removes the unneeded initializer and eliminated a warning message from compiling the code, preventing this error.

BZ#691760

The testcase **`systemtap.stress/conversions.exp`** had 3 FAILs. This was because PR12168 eliminated duplicated error messages and changed the count of ERROR and WARNING messages. This patch adds the **`-vv`** option which turns off the duplication eliminate and allows an accurate count of the number of times ERROR and WARNING messages occurred, preventing these errors.

BZ#692869

The testcases **`systemtap.examples/process/errsnoop build`**, **`buildok/syscall.stp`**, and **`buildok/syscalls2-detailed.stp`** failed to build with a semantic error. This patch checks for the existence of dwarf variables instead of using CONFIG_NFSD, which allows these testcases to

build successfully.

1.282.4. RHBA-2011:1150 — systemtap bug fix update

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

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.

Bug Fixes

BZ#725809

When the system ran out of memory in a module, systemtap failed to remove the module directory created by the debugfs debugger. Consequently, systemtap was unable to load the same module until after a system reboot; sometimes even a kernel panic occurred. With this update, a patch has been provided to address this issue, and systemtap now properly removes the module directory in the described scenario, thus fixing this bug.

BZ#726051

Under unusual circumstances, the rate of error or warning messages sent from the probe module to userspace exceeded various buffers. As a consequence, some control messages were sometimes lost which eventually led to a kernel panic in some cases. With this update, the transport layer ensures that all control messages are delivered even if there is a flood of warning or error messages, thus fixing this bug.

Affected systemtap users should upgrade to these updated packages, which fix these bugs.

1.283. sysvinit-tools

1.283.1. RHBA-2011:0698 — sysvinit-tools bug fix update

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

The sysvinit-tools package contains various tools used for process management.

Bug Fixes

BZ#619658

Previously, the wall(1) command incorrectly allowed to send 22 lines per message at once. This update sets the wall(1) command to reflect accurately the maximum of 20 lines per message.

BZ#668476

Previously, parts of the banner message got cut off when the host name was longer than expected and the banner limit of 80 characters was exceeded. This update allows also for longer host names. Now, the banner no longer gets cut off.

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

1.284. tcsh

1.284.1. RHBA-2011:0193 — tcsh bug fix update

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

Tcsh is an enhanced and compatible version of the C shell (csh). It is a command language interpreter, which can be used as an interactive login shell, as well as a shell script command processor.

Bug Fixes

BZ#658171

Previously, running tcsh in verbose mode (that is, by using the "-v" option) caused the shell to append history to its output on exit. With this update, a patch has been applied to address this issue, and tcsh now works as expected.

BZ#669176

On a local machine, tcsh set the "REMOTEHOST" environment variable to an empty string, even though this variable should be only set on remote machines. This error has been fixed, and "REMOTEHOST" is no longer set on a local machine.

BZ#673556

Previously, when command substitution with backquotes was used, extra fork() was performed. With this update, only one fork() is performed.

All users of tcsh are advised to upgrade to this updated package, which resolves these issues.

1.285. thunderbird

1.285.1. RHSA-2011:0886 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-2377

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.

CVE-2011-0083, **CVE-2011-0085**, **CVE-2011-2363**

Multiple dangling pointer flaws were found in Thunderbird. Malicious HTML content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2011-2364, **CVE-2011-2365**, **CVE-2011-2374**, **CVE-2011-2375**, **CVE-2011-2376**

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-2011-2362

It was found that Thunderbird could treat two separate cookies (for web content) as interchangeable if both were for the same domain name but one of those domain names had a trailing "." character. This violates the same-origin policy and could possibly lead to data being leaked to the wrong domain.

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.

1.285.2. RHSA-2011:1166 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-2982

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-2011-0084

A dangling pointer flaw was found in the Thunderbird Scalable Vector Graphics (SVG) text manipulation routine. An HTML mail message containing a malicious SVG image could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2011-2378

A dangling pointer flaw was found in the way Thunderbird handled a certain Document Object Model (DOM) element. 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.

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.

1.285.3. RHSA-2011:1243 — Important: thunderbird security update

An updated thunderbird 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.

Mozilla Thunderbird is a standalone mail and newsgroup client.

It was found that a Certificate Authority (CA) issued a fraudulent HTTPS certificate. This update renders any HTTPS certificates signed by that CA as untrusted, except for a select few. The now untrusted certificates that were issued before July 1, 2011 can be manually re-enabled and used again at your own risk in Thunderbird; however, affected certificates issued after this date cannot be re-enabled or used. (BZ#734316)

All Thunderbird users should upgrade to this updated package, which resolves this issue. All running instances of Thunderbird must be restarted for the update to take effect.

1.285.4. RHSA-2011:1267 — Important: thunderbird security update

An updated thunderbird 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.

Mozilla Thunderbird is a standalone mail and newsgroup client.

The RHSA-2011:1243 Thunderbird update rendered HTTPS certificates signed by a certain Certificate Authority (CA) as untrusted, but made an exception for a select few. This update removes that exception, rendering every HTTPS certificate signed by that CA as untrusted. (BZ#735483)

All Thunderbird users should upgrade to this updated package, which resolves this issue. All running instances of Thunderbird must be restarted for the update to take effect.

1.285.5. RHSA-2011:1342 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-2995

Several flaws were found in the processing of malformed HTML 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-2011-2372

A flaw was found in the way Thunderbird processed the "Enter" keypress event. A malicious HTML mail message could present a download dialog while the key is pressed, activating the default "Open" action. A remote attacker could exploit this vulnerability by causing the mail client to open malicious web content.

CVE-2011-3000

A flaw was found in the way Thunderbird handled Location headers in redirect responses. Two copies of this header with different values could be a symptom of a CRLF injection attack against a

vulnerable server. Thunderbird now treats two copies of the Location, Content-Length, or Content-Disposition header as an error condition.

CVE-2011-2999

A flaw was found in the way Thunderbird handled frame objects with certain names. An attacker could use this flaw to cause a plug-in to grant its content access to another site or the local file system, violating the same-origin policy.

CVE-2011-2998

An integer underflow flaw was found in the way Thunderbird handled large JavaScript regular expressions. An HTML mail message containing malicious JavaScript could cause Thunderbird to access already freed memory, causing 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.

1.285.6. RHSA-2011:1439 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple security issues is now available for Red Hat Enterprise Linux 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-3647

A flaw was found in the way Thunderbird handled certain add-ons. Malicious, remote content could cause an add-on to elevate its privileges, which could lead to arbitrary code execution with the privileges of the user running Thunderbird.

CVE-2011-3648

A cross-site scripting (XSS) flaw was found in the way Thunderbird handled certain multibyte character sets. Malicious, remote content could cause Thunderbird to run JavaScript code with the permissions of different remote content.

CVE-2011-3650

A flaw was found in the way Thunderbird handled large JavaScript scripts. Malicious, remote content 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.

1.286. tigervnc

1.286.1. RHSA-2011:0871 — Moderate: tigervnc security update

Updated tigervnc 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.

Virtual Network Computing (VNC) is a remote display system which allows you to view a computer's desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. TigerVNC is a suite of VNC servers and clients.

Security Fix

CVE-2011-1775

It was discovered that vncviewer could prompt for and send authentication credentials to a remote server without first properly validating the server's X.509 certificate. As vncviewer did not indicate that the certificate was bad or missing, a man-in-the-middle attacker could use this flaw to trick a vncviewer client into connecting to a spoofed VNC server, allowing the attacker to obtain the client's credentials.

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

1.286.2. RHBA-2011:0649 — tigervnc bug fix and enhancement update

Updated tigervnc packages that fix several bugs and add an enhancement are now available.

Virtual Network Computing (VNC) is a remote display system which allows you to view a computing desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. TigerVNC is a suite of VNC servers and clients.

Bug Fixes

BZ#588342

Xvnc could become unresponsive and the following error message was shown in the log: "[mi] EQ overflowing. The server is probably stuck in an infinite loop.". This was caused by a large number of user input events in the Xvnc event queue, which were being processed too slowly. With this update, this issue no longer occurs and the system works as expected.

BZ#628054

Prior to this update, Xvnc (the X VNC server; part of the tigervnc package) did not pass keyboard input to a remote VMware workstation because it did not take into account types of keyboards which do not have modifier keys. With this update, Xvnc recognizes all types of keyboards; thus, keyboard input is correctly passed to remote VMware workstations.

BZ#632530

When connecting to a remote machine, the default ".vnc/xstartup" file did not load the i18n (the default X locale settings) settings from the "/etc/sysconfig/i18n" file which caused the remotely accessed desktop to always use the "en_US" locale. With this update, the default ".vnc/xstartup" file loads the i18n settings and shows the correct locale.

BZ#634161

The tigervnc-server package was missing a perl dependency, causing the "/usr/bin/vncserver" script to fail to run. This update adds the perl dependency to the tigervnc-server package; thus, the "/usr/bin/vncserver" script runs as expected.

BZ#645755

The Xvnc server randomly refused connections when the reading of the password file (provided when starting Xvnc with the "-PasswordFile" option) was interrupted by a signal. With this update, the loading of a password file continues after an interrupt signal is issued and connections are no longer refused.

Enhancement

BZ#653491

TigerVNC (Xvnc, x0vncserver, the libvnc.so module, and vncviewer) now supports TLS encryption (using VeNCrypt) which allows TLS encrypted communication between a server and a viewer.

Users are advised to upgrade to these updated tigervnc packages, which resolve these issues and add this enhancement.

1.287. tomcat6

1.287.1. RHSA-2011:0791 — Moderate: tomcat6 security and bug fix update

Updated tomcat6 packages that fix three 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Security Fixes

CVE-2010-3718

It was found that web applications could modify the location of the Tomcat host's work directory. As web applications deployed on Tomcat have read and write access to this directory, a malicious web application could use this flaw to trick Tomcat into giving it read and write access to an arbitrary directory on the file system.

CVE-2010-4172

A cross-site scripting (XSS) flaw was found in the Manager application, used for managing web applications on Tomcat. If a remote attacker could trick a user who is logged into the Manager application into visiting a specially-crafted URL, the attacker could perform Manager application tasks with the privileges of the logged in user.

CVE-2011-0013

A second cross-site scripting (XSS) flaw was found in the Manager application. A malicious web application could use this flaw to conduct an XSS attack, leading to arbitrary web script execution with the privileges of victims who are logged into and viewing Manager application web pages.

Bug Fixes

BZ#636997

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.

BZ#661244

The "/usr/share/java/" directory was missing a symbolic link to the "/usr/share/tomcat6/bin/tomcat-juli.jar" library. Because this library was mandatory for certain operations (such as running the Jasper JSP precompiler), the "build-jar-repository" command was unable to compose a valid classpath. With this update, the missing symbolic link has been added.

BZ#678671

Previously, the "tomcat6" init script failed to start Tomcat with a "This account is currently not available." message when Tomcat was configured to run under a user that did not have a valid shell configured as a login shell. This update modifies the init script to work correctly regardless of the daemon user's login shell. Additionally, these new tomcat6 packages now set "/sbin/nologin" as the login shell for the "tomcat" user upon installation, as recommended by deployment best practices.

BZ#643809

Some standard Tomcat directories were missing write permissions for the "tomcat" group, which could cause certain applications to fail with errors such as "No output folder". This update adds write permissions for the "tomcat" group to the affected directories.

BZ#695284, BZ#697504

The "/usr/sbin/tomcat6" wrapper script used a hard-coded path to the "catalina.out" file, which may have caused problems (such as for logging init script output) if Tomcat was being run with a user other than "tomcat" and with CATALINA_BASE set to a directory other than the default.

BZ#698624

Stopping Tomcat could have resulted in traceback errors being logged to "catalina.out" when certain web applications were deployed.

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.

1.287.2. RHSA-2011:1780 — Moderate: tomcat6 security and bug fix update

Updated tomcat6 packages that fix several 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Security Fixes

CVE-2011-1184

APR (Apache Portable Runtime) as mentioned in the CVE-2011-3190 and CVE-2011-2526 descriptions does not refer to APR provided by the apr packages. It refers to the implementation of APR provided by the Tomcat Native library, which provides support for using APR with Tomcat. This library is not shipped with Red Hat Enterprise Linux 6. This update includes fixes for users who have elected to use APR with Tomcat by taking the Tomcat Native library from a different product. Such a configuration is not supported by Red Hat, however.

Multiple flaws were found in the way Tomcat handled HTTP DIGEST authentication. These flaws weakened the Tomcat HTTP DIGEST authentication implementation, subjecting it to some of the weaknesses of HTTP BASIC authentication, for example, allowing remote attackers to perform session replay attacks.

CVE-2011-3190

A flaw was found in the way the Coyote (org.apache.coyote.ajp.AjpProcessor) and APR (org.apache.coyote.ajp.AjpAprProcessor) Tomcat AJP (Apache JServ Protocol) connectors processed certain POST requests. An attacker could send a specially-crafted request that would cause the connector to treat the message body as a new request. This allows arbitrary AJP messages to be injected, possibly allowing an attacker to bypass a web application's authentication checks and gain access to information they would otherwise be unable to access. The JK (org.apache.jk.server.JkCoyoteHandler) connector is used by default when the APR libraries are not present. The JK connector is not affected by this flaw.

CVE-2011-2204

A flaw was found in the Tomcat MemoryUserDatabase. If a runtime exception occurred when creating a new user with a JMX client, that user's password was logged to Tomcat log files. Note: By default, only administrators have access to such log files.

CVE-2011-2526

A flaw was found in the way Tomcat handled sendfile request attributes when using the HTTP APR or NIO (Non-Blocking I/O) connector. A malicious web application running on a Tomcat instance could use this flaw to bypass security manager restrictions and gain access to files it would otherwise be unable to access, or possibly terminate the Java Virtual Machine (JVM). The HTTP blocking IO (BIO) connector, which is not vulnerable to this issue, is used by default in Red Hat Enterprise Linux 6.

Red Hat would like to thank the Apache Tomcat project for reporting the CVE-2011-2526 issue.

Bug Fix

BZ#748807

Previously, in certain cases, if "LANG=fr_FR" or "LANG=fr_FR.UTF-8" was set as an environment variable or in "/etc/sysconfig/tomcat6" on 64-bit PowerPC systems, Tomcat may have failed to start correctly. With this update, Tomcat works as expected when LANG is set to "fr_FR" or "fr_FR.UTF-8".

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.

1.288. tuned

1.288.1. RHBA-2011:0581 — tuned bug fix and enhancement update

Updated tuned packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

The tuned packages contain a daemon that tunes system settings dynamically. It does so by monitoring the usage of several system components periodically.

The tuned packages have been upgraded to upstream version 0.2.18, which provides a number of bug fixes and enhancements over the previous version. (BZ#661715)

Bug Fixes

BZ#636548

For device mapper and multipath devices used on the system, I/O scheduler changes in tuned were not applied on these devices. This bug affected several tuned profiles. To fix this bug, device mapper devices have been added into the list of tuned devices and the I/O scheduler changes are now applied on device mapper devices as well.

BZ#658843

Read-ahead in tuned was not set correctly, nor was it set it for all appropriate logical unit numbers (LUNs). As a consequence, devices mapped with the device mapper could not be handled. Now, instead of setting static read-ahead value for all devices, the previous value is multiplied and tuned sets an acceptable read-ahead value for all disks including device mapper devices.

BZ#621122

When the tuned script terminated unexpectedly, "service tuned status" returned exit code 2 while it should have been 1; the presence of the pidfile was not checked correctly. With this update, this bug has been fixed and a tuned status check will now return correct status code when it crashes.

BZ#624494

When the tuned daemon was enabled on an IBM S/390 system, due to its hardware limitations, plug-ins for CPU and disk did not work at all and the network plug-in made very little difference to be useful. Architecture compatibility check has been integrated into tuned; the daemon is now disabled and will not start on IBM S/390.

BZ#689715

When parsing an unsupported network card link mode, tuned terminated unexpectedly. With this update, a fix has been provided to address this bug and the crash no longer occurs.

BZ#682380

Previously, the network device naming scheme in tuned assumed all Ethernet devices were named "ethX". This was non-compliant with the naming convention for network interfaces in Red Hat Enterprise Linux 6, which introduces new names for network ports with respect to their usage or user-defined labels. With this update, tuned supports different names for Ethernet cards and users of tuned network plug-in can recognize their cards as configured in their tuned.conf file.

BZ#625850

Previously, four executables (diskdevstat, netdevstat, scomes, varnetload) were missing man pages. With this update, the man pages have been added.

BZ#619812

Previously, man pages for tuned included inaccuracies in the profile descriptions and descriptions for several plug-ins were missing. This update corrects these inaccuracies and adds the plug-in descriptions to the tuned man pages.

Enhancement

BZ#643462

This update introduces new udev rules and other settings to configure non-SATA devices separately from SATA devices. Now, when a user installs tuned, the default configuration is optimized for non-SATA devices.

Users of tuned are advised to upgrade to these updated packages which fix these bugs and add this enhancement.

1.289. udev

1.289.1. RHSA-2011:0525 — udev bug fix and enhancement update

New udev packages that fix a number of bugs and adds an enhancement, are now available for Red Hat Enterprise Linux 6.

The udev packages implement a dynamic device-directory, providing only the devices present on the system. This dynamic directory runs in userspace, dynamically creates and removes devices, provides consistent naming, and a userspace API. udev replaces devfs, providing greater hot plug functionality.

Bug Fixes

BZ#617572

The kernel recognizes key press events that tell it that a key has been pressed, and key release events that tell it that the key has been released and that the user is not holding the key down. Previously, keyboard keys for advanced functions, like volume control would sometimes produce key press events without corresponding key release events, which the kernel interpreted as the key being held down, even though the user had released the key. This update sets the **`force key release`** for these advanced function keys so that the keys behave as expected and unwanted key repeats no longer occur.

BZ#644902

In previous versions of udev, the **`scsi_id`** command only queried one sort of page id and returned either the id of page **`0x80`** or **`0x83`** was used for **`ID_SERIAL_RAW`**. To query the other id, another run of **`scsi_id`** was needed. This update adds two new options to the ***`--page=`*** page code argument: **`0x80-0x83`** and **`0x83-0x80`**. Both export **`ID_SERIAL_80`** and **`ID_SERIAL_83`**:

- For **`0x80-0x83`**, **`ID_SERIAL_SHORT`** always equals **`ID_SERIAL_80`**.

  For **`0x83-0x80`**, **`ID_SERIAL_SHORT`** always equals **`ID_SERIAL_83`**.

You must modify **`/etc/scsi_id.config`** to change the default page code.

Example usage:

```
# scsi_id --export --page=0x80-0x83 --whitelisted /dev/sdc|grep
```

```
ID_SERIAL_
ID_SERIAL_RAW="SATA     SAMSUNG HD400LDS0AXJ1LL903246      "
ID_SERIAL_80=SATA_SAMSUNG_HD400LDS0AXJ1LL903246
ID_SERIAL_SHORT=S0AXJ1LL903246
ID_SERIAL_83=1ATA_SAMSUNG_HD400LD_S0AXJ1LL903246
```

BZ#647794

In a virtual machine with an iDRAC virtual CDROM, the CDROM could not be mounted from the desktop, because **/lib/udev/cdrom_id** failed to get the correct information about the drive and medium. In this update, **/lib/udev/cdrom_id** has been fixed to correctly read information about the drive and medium of an iDRAC virtual drive.

BZ#656059

Previously, some dynamic ethernet interfaces with zero MAC addresses were erroneously added to the list of persistent interfaces in **/etc/udev/rules.d/70-persistent-net.rules**. This resulted network interfaces being named incorrectly. In this updated package, these interfaces are no longer listed as persistent, which corrects the naming problem.

BZ#657360

Previously, the option **udevadm trigger** caused a segmentation fault when **udevadm** if debugging was turned on in **/etc/udev.conf**. With this update, this option **udevadm trigger** behaves as expected and the segmentation fault does not occur.

BZ#660367

Virtual CDROM or DVD media presented through an iDRAC card were not recognized correctly by **udev** helpers. As a result, attempts to install from such a medium would fail. This updated udev package provides a corrected **cdrom_id** which now works with iDRAC cards.

BZ#663064

Previously, the autosuspend feature of qemu virtual mouse, tablet and keyboard devices were not available in the sysfs representation of these devices. It was not therefore possible to detect when such devices were not in use and to autosuspend the virtual machines to which they were attached. This release of **udev** turns on the autosuspend feature of these devices to reduce load on virtual machines without the need for manual interaction by the sysadmin.

BZ#667750

In previous releases, **/dev/hugepages** was not created by **udev** and therefore could not be mounted automatically. This directory is now created in the **start_udev** script after **/dev** is mounted.

BZ#674168

In previous versions of the udev rules it was not possible to turn off console user ownership of certain devices. For example, if you want to remove console ownership of the CDROM device in a udev rule with:

```
SUBSYSTEM=="block", ENV{ID_CDROM}=="1", ENV{ACL_MANAGE}="0"
```

the **ENV{ACL_MANAGE}="0"** was not completly honored.

This update fixes **udev-acl** tool, which is part of **udev**, to honor **0** as a setting

BZ#676004

Previously, the **udevd** daemon was not compiled with the **PIE** and **RELRO** flags, so the daemon was missing some security mechanisms available. This update release fixes the issue.

BZ#677857

A memory allocation issue could cause previous versions of **udevadm trigger** to fail with a segmentation fault when a device was delayed. In this release, the memory allocation issue is corrected, and **udevadm trigger** does not fail when devices are delayed.

BZ#687956

Some virtual machines do not properly implement the **READ TOC** SCSI command. On such virtual machgines, the Red Hat Enterprise Linux installer (**anaconda**) could not recognize the DVD medium properly. These updated udev packages include a workaround in **cdrom_id** which allow virtual machines with faulty implementations of the **READ TOC** SCSI command to recognize DVDs.

Enhancements

BZ#644330

Previously, the output of the command **udevadm info --query=property** could not be used as input to shell interpreters. This update adds an **--export** argument so that the output of **udevadm info --query=property --option** is parsable by the shell.

Users of udev should upgrade to these updated packages, which fix these bugs and add this enhancement.

1.290. upstart

1.290.1. RHBA-2011:0531 — upstart bug fix update

An updated upstart package that fixes various bugs is now available.

upstart is an event-based replacement for the /sbin/init daemon that starts tasks and services during boot, stops them during shut down, and supervises them while the system is running.

Bug Fixes

BZ#648431

Calling /sbin/telinit resulted in a failed assertion on the 64-bit IBM POWER Series because the value of telinit's "ret" variable was not initialized when it was declared. The value of "ret" is now set explicitly when the variable is declared.

BZ#618995

upstart sends jobs to the shell via a pipe represented by the file descriptors under /proc/self/fd/ in the /proc filesystem. One of these file descriptors was not closed, which resulted in a message about a file descriptor leak when operating at run level 1. This file descriptor is now closed correctly.

BZ#633216

upstart did not update the relevant entry in /var/run/utmp when a mingetty session was terminated. This resulted in user process entries being shown for terminals that were no longer active. The relevant entry in /var/run/utmp is now correctly set to "DEAD_PROCESS" when a mingetty session is terminated.

BZ#676002

The upstart package is now built with PIE and RELRO flags in order to comply with Common Criteria specifications.

All users are advised to upgrade to this updated package, which resolves these issues. Note that after installing this update, a system reboot is required for the above changes to take effect.

1.291. util-linux-ng

1.291.1. RHSA-2011:0699 — util-linux-ng bug fix and enhancement update

Updated util-linux-ng packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The util-linux-ng packages contain a large variety of low-level system utilities that are necessary for a Linux operating system to function.

Bug Fixes

BZ#561111

The **context=**, **defcontext=**, **fscontext=**, and **rootcontext=** options should not be used for remount operations. Prior to this update, using these options when remounting a manually mounted volume could cause the **mount** utility to fail with an error message similar to the following:

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

This update applies an upstream patch that disables the **context=**, **defcontext=**, **fscontext=**, and **rootcontext=** options when remounting a file system, and manually mounted volumes can now be remounted as expected.

BZ#615389

When used to list the currently attached file systems, the previous version of the **mount** utility did not display information about the mapping of loop devices. With this update, the underlying source code has been adapted to address this issue, and **mount** now displays the loop device mapping as expected.

BZ#616393

When mounting the **tmpfs** file system, the previous version of the **mount** utility incorrectly required **root** privileges even when the corresponding entry in the **/etc/fstab** file contained the **user** option. Consequent to this, an attempt to mount such a file system as a non-root user failed with the following error:

```
mount: only root can do that
```

This update corrects an error in the **mount.tmpfs** wrapper that prevented non-root users from mounting the **tmpfs** file system. As a result, the **mount** utility no longer requires **root** privileges when the **user** option is specified in **/etc/fstab**.

BZ#619139

Under certain circumstances, the **fsck** utility may have failed to exit with a non-zero exit status when it encountered an error. This update applies an upstream patch, which ensures that a proper exit status is used when the **fsck** utility fails.

BZ#621312

Prior to this update, running the **losetup** utility with the **--help** (or **-h**) command line option caused the utility to return exit status **1**, even though it successfully displayed the usage information. This error has been fixed, and **losetup** now correctly terminates with exit status **0** in this situation.

BZ#623012

Previously, the presence of an offline CPU caused the **lscpu** utility to fail with an error message similar to the following:

```
lscpu: error: cannot open
/sys/devices/system/cpu/cpu1/cache/index0/shared_cpu_map: No such file
or directory
```

With this update, an upstream patch has been applied to address this issue, and **lscpu** now produces the expected output.

BZ#624521

Due to incorrect translation of partition names to whole-disk names, the **fsck** utility may have failed to process file systems on multiple physical disk drives in parallel. This update applies an upstream patch that ensures the partition names are translated to the whole-disk names correctly. As a result, **fsck** now processes file systems on multiple physical disk drives in parallel as expected.

BZ#625064

Prior to this update, the **mount** and **umount** utilities did not support file system subtypes. Consequent to this, when the FUSE (Filesystem in Userspace) module was in use, non-root users were unable to unmount SSHFS file systems, even when the **user** option was specified in the **/etc/fstab** file. This update adapts the **mount** and **umount** utilities to provide support for file system subtypes (that is, in the ***type.subtype*** form). As a result, non-root users are now allowed to unmount the **fuse.sshfs** file systems as expected.

BZ#626374

Prior to this update, the **fdisk** utility incorrectly verified alignment of logical sectors with a size other than 512 bytes. Consequent to this, when a user issued the **p** command to display the partition table, he may have been presented with a message similar to the following:

```
Partition 1 does not start on physical sector boundary.
```

With this update, a patch has been applied to address this issue, and **fdisk** now works as expected.

BZ#644503

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.

BZ#650879

When running the **column** utility with the **-t** command line option, an attempt to use the same character on standard input and as an argument of the **-s** option caused the utility to terminate unexpectedly with a segmentation fault. With this update, a patch has been applied to address this issue, and the **column** utility no longer crashes.

BZ#650953

Previously, the **wipefs** utility did not erase Linux Unified Key Setup (LUKS) signatures. This update corrects this error, and **wipefs** now removes the LUKS signatures as expected.

BZ#656453

Previously, the **libblkid** library incorrectly re-validated cache entries. This error has been fixed, and **libblkid** now works correctly.

BZ#663731

When listing partition tables, the **fdisk -l** and **sfdisk -d** commands incorrectly listed multipath devices in the **/dev/dm-*number*** form. This update corrects this error, and both commands now list multipath devices in the **/dev/mapper/mpath*number*** form as expected.

BZ#670770

Prior to this update, the **lscpu** utility failed to identify 32-bit support on 64-bit AMD processors, and only listed the 64-bit support in the **CPU op-mode(s)** field. With this update, the underlying source code has been modified to address this issue, and **lscpu** now lists 32-bit capabilities of 64-bit AMD processors as expected.

BZ#678306

Prior to this update, the **libuuid** library did not provide a safe variant of the **uuid_generate_time()** function. Under certain circumstances, this may have caused the **uuidd** service to generate duplicate UUIDs (universally unique identifiers). This update applies a series of patches that introduce a safe variant of the **uuid_generate_time()** function. As a result, the **uuidd** service now always generates unique UUIDs.

BZ#678378

Various parts of the underlying source code have been adapted to comply with the Common Criteria requirements.

BZ#612325

The “SEE ALSO” section of the **mkfs**(8) manual page has been extended to include a reference to **mkfs.ext4**(8).

BZ#651035

Prior to this update, the “Mount options for cifs” section of the **mount**(8) manual page stated that the **mount.cifs**(8) manual page is provided by the samba-client package. However, this manual page is

now included in the cifs-utils. This update corrects the **mount**(8) manual page to refer to the correct package.

BZ#665376

Previously, the **mount**(8) manual page did not provide an accurate description of the `atime` mount option. This update corrects this error, and the **mount**(8) manual page now describes the `atime` option properly.

BZ#671357

Previous version of the **mount**(8) manual page did not describe some of the mount options that are available for the `ext3` and `ext4` file systems. This update corrects the “Mount options for ext3” and “Mount options for ext4” sections of the manual page to include descriptions of all available `ext3` and `ext4` mount options as expected.

Enhancements

BZ#616325

This update adds the **findmnt** utility to Red Hat Enterprise Linux 6. The **findmnt** utility allows users to list all mounted file systems in a tree-like format, or display information about a particular mount.

BZ#657082

This update adds the **lsblk** utility to Red Hat Enterprise Linux 6. The **lsblk** utility allows users to list block devices and their attributes in a tree-like format.

All users of util-linux-ng are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.292. valgrind

1.292.1. RHBA-2011:0665 — valgrind bug fix and enhancement update

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

Valgrind is a tool to help users find memory management problems in the programs. Valgrind can detect a lot of problems that are otherwise very hard to find or diagnose.

The valgrind packages have been upgraded to upstream version 3.6.0, which provides several bug fixes and enhancements over the previous version. (BZ#661245)

Bug Fixes

BZ#679906

When MySQL Server was run via valgrind, an error in valgrind prevented MySQL Server from writing to its log file and caused it to return a number of error messages. This bug has been fixed and MySQL Server now starts up normally when run via valgrind.

BZ#665289

When the snmpd tool was executed under valgrind on the 64-bit PowerPC architecture, it terminated unexpectedly. This bug has been fixed and the "valgrind /usr/sbin/snmpd" command now works as expected.

Enhancements

BZ#630173

With this update, valgrind now supports IBM POWER 6 and IBM POWER 7 systems.

BZ#632354

With this update, valgrind now supports IBM System z.

Users of valgrind are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.293. vgabios

1.293.1. RHBA-2011:0776 — vgabios bug fix update

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

The vgabios package provides is an GNU Lesser General Public License (LPGL) implementation of a BIOS for a video card. The vgabios package contains BIOS images that are intended to be used in the Kernel Virtual Machine (KVM).

Bug Fixes

BZ#654639

Previously, the vgabios for the qemu standard vga expected to find the framebuffer memory at the magic address 0xe0000000. Due to the overlapping memory reservations, qemu-kvm aborted unexpectedly when the guest operating system (OS) tried to use the address space at 0xe0000000 for other spaces, e.g. mapping resources of hot-plugged PCI devices. This update changes the vgabios to lookup the framebuffer memory in PCI space instead. Now, the address space at 0xe0000000 can freely be used by the guest OS.

BZ#691344

Previously, vgabios did not support DOS Protected Mode Services (DPMS) for Amazon Simple Storage Service (Amazon S3) for Windows guests. This update adds DPMS support.

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

1.294. vim

1.294.1. RHBA-2011:0297 — vim bug fix update

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

Vim (Vi IMproved) is an updated and improved version of the vi editor.

Bug Fix

BZ#629568

When editing a shell script (that is, "filetype=sh"), the presence of the "\c" escape sequence followed by a non-space character caused syntax highlighting to incorrectly report a syntax error. With this update, the relevant regular expression in the syntax file has been corrected, and syntax is now highlighted as expected.

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

1.295. virt-manager

1.295.1. RHBA-2011:0637 — virt-manager bug fix and enhancement update

An updated virt-manager package that provides bug fixes and adds enhancements is now available for Red Hat Enterprise Linux 6.

Virtual Machine Manager (virt-manager) is a graphical tool for administering virtual machines for KVM, Xen, and QEMU. virt-manager can start, stop, add or remove virtualized devices, connect to a graphical or serial console, and view resource usage statistics for existing virtualized guests on local or remote machines. It uses the libvirt API.

The virt-manager package has been upgraded to upstream version 0.8.6, which provides a number of bug fixes and enhancements over the previous version.

Bug Fixes

BZ#619894

Previously, if selecting 'Customize before install' at the end of the 'New VM' wizard and the install process failed, any custom changes made were forgotten if the installation was re-run. This is now fixed.

BZ#640781

Previously, the 'New VM' wizard incorrectly capped maximum guest memory at 32GB. This limitation has been removed.

Enhancements

BZ#647306

Option to configure guest CPU model, including an option to mimic host CPU in the guest, which can greatly improve performance.

BZ

Option to configure CPU topology (sockets, cores, threads). This enables using more CPUs with OS which have a support limit on sockets (the default vcpu type).

BZ

Cancellation and progress reporting for 'Save' and 'Migrate' operations.

BZ#613546

Option to see the error message if a hotplug operation fails. This can be useful in determining if hotplug for the specified device type is supported and failure was expected.

BZ

Use of ICH6 sound device model by default.

All users of Red Hat Enterprise Linux 6 should upgrade to these updated packages.

1.296. virt-top

1.296.1. RHBA-2011:0720 — virt-top bug fix update

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

virt-top is a utility like top(1) for displaying virtualization stats.

Bug Fixes

BZ#605124

On the PowerPC platform, binary files generated by the OCaml compiler were running with executable stacks. As this was not a necessary or desirable behavior, Exec-Shield stack protection has been enabled for the file usr/bin/virt-top. Binary files generated by the OCaml compiler no longer run with executable stacks.

BZ#629500

The "historical %CPU" was displayed at the bottom of virt-top's output, whereas the virt-top(1) manual page indicated that it was placed at the top of virt-top's display. This update corrects virt-top's output so that the "historical %CPU" is now correctly displayed in the top right-hand corner of virt-top's output, thus resolving the issue.

BZ#634435

When a user randomly changed the size of the terminal window in which the virt-top utility was running, virt-top aborted unexpectedly. This update corrects the behavior so that virt-top no longer aborts unexpectedly when resizing the terminal window.

BZ#648186

Previously, the virt-top manual page referenced the xm and xentop utilities of Xen. Because Red Hat no longer ships these utilities with Red Hat Enterprise Linux 6, the references in the virt-top manual page have been removed. The manual page no longer mentions the Xen utilities that are not available in Red Hat Enterprise Linux 6.

BZ#676979

The virt-top(1) manual page and help option incorrectly indicated that Xen was the default hypervisor. This update corrects the virt-top manual page and help option to remove the incorrect indications.

BZ#661783

The virt-top utility previously required the ocaml-camomile-data package in order to be built. Because the ocaml-camomile-data package is not present in Red Hat Enterprise Linux 6, and is actually not a requirement for building the virt-top package, this dependency has been dropped. This updated virt-top package no longer requires the ocaml-camomile-data as a dependency.

BZ#637964

When a user used the "--end-time" option of the virt-top utility, the specified execution time was not

followed. Instead, the "--end-time" option gave inaccurate results due to the erroneous computing of timezones. The issue has been resolved by fixing the problem. Now the "--end-time" option works correctly and provides expected output.

BZ#680344

When using the "--end-time" option of the virt-top utility, the utility did not stop at the time specified. Instead, the utility continued in execution. This has been caused by virt-top not following user's local timezones and making use of UTC instead. The problem has been fixed so that virt-top now uses local timezones and stops at the time specified by the user.

BZ#647991

Previously, the virt-top(1) manual page did not give correct information on virtual machine's memory usage when running in batch mode. It did not mention the fact that the virt-top utility only shows the memory allocated to the guest, not the real amount of memory used by the guest. This misleading information has been corrected and the virt-top utility manual page no longer confuses the user.

BZ#643893

Previously, the virt-top's option "-b" as documented in the virt-top manual page did not work as expected. The results of the "virt-top -b" and "virt-top" commands were the same. The issue has been resolved by making virt-top's behavior in batch mode similar to the command "top -b". Now virt-top works correctly in batch mode.

All users of virt-top should install these updated packages, which resolve these issues.

1.297. virt-v2v

1.297.1. RHSA-2011:0650 — virt-v2v bug fix and enhancement update

Updated virt-v2v and augeas packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

virt-v2v is a tool for converting virtual machines to use the KVM hypervisor. It modifies both the virtual machine image and its associated libvirt metadata. virt-v2v will also configure a guest to use VirtIO drivers if possible.

augeas is a library for programmatically editing configuration files. augeas parses configuration files as a tree structure, which it exposes through its public API.

Bug Fixes

BZ#609483

Red Hat Enterprise Linux guest conversion did not update **`/etc/sysconfig/kernel`**, which would lead to an incorrect kernel being set as the default in future updates. This would cause boot failure. **`/etc/sysconfig/kernel`** now updates correctly.

BZ#616720

Partially written guest images were not cleaned up if a conversion to a libvirt target failed or was interrupted. With this update, all created volumes are removed if a conversion is not successful.

BZ#618965

virt-v2v would not always update software in the transfer volume when updates were available because it relied on timestamps. The transfer volume is now updated whenever virt-v2v is used.

BZ#623571

virt-v2v could not detect VMware Tools to uninstall it if VMware Tools was installed via tarball. When VMware Tools detected that it was no longer running on a VMware platform and attempted to disable itself on the guest, it overwrote changes made by virt-v2v during conversion. This resulted in broken networking and initrd images containing unnecessary drivers. virt-v2v can now detect and uninstall VMware Tools even when VMware Tools is installed via tarball.

BZ#623579

If a Linux guest had an invalid default entry in the **`grub.conf`** file, virt-v2v assumed it was an i686 guest. This resulted in a converted guest that did not boot. virt-v2v now assumes an AMD64 or Intel 64 default architecture instead of i686.

BZ#642258

virt-v2v could not convert a Red Hat Enterprise Linux guest that did not have the **`/etc/securetty`** file. Conversion without this file is now possible.

BZ#643867

Conversion failed if conversion required updating the kernel and the guest had additional kernel modules installed. Conversion now succeeds and virt-v2v no longer attempts to uninstall old kernels.

BZ#644295

When performing an offline installation of the VirtIO block driver in a Windows guest, virt-v2v incorrectly assumed that **`ControlSet001`** was always the current control set, even if **`ControlSet001`** had been marked as failed. The correct control set is now detected, and the VirtIO block driver installed in the correct location.

BZ#656883

When creating a libvirt guest using block storage, virt-v2v incorrectly set the disk type to **`auto`**. This made libvirt unable to start the guest. Disk type is now set explicitly based on source metadata or other detection methods.

BZ#581421

In certain circumstances, virt-v2v exited with a return value of **`0`**, even though conversion failed. The correct values are now returned.

BZ#609448

Red Hat Enterprise Linux guest conversion did not update **`/boot/grub/device.map`** with converted block device names in certain circumstances. **`device.map`** now updates as expected.

BZ#670778

virt-v2v failed to convert a guest to a Red Hat Enterprise Virtualization target if the current working directory was not universally readable. Universal readability is no longer required.

BZ#672521

virt-v2v failed to convert Windows guests that had a **C:\Temp** directory because it created a **C:\temp** directory without checking for file names that used alternative cases. virt-v2v now checks for case-sensitive file names before creating an appropriate temporary directory.

BZ#671300

virt-v2v failed to enable VirtIO support when converting a Xen guest that had both a paravirtualized Xen kernel and a fully virtualized kernel installed. The fully virtualized kernel is now made the default kernel and conversion succeeds as expected.

BZ#676323

It was not possible to create a Red Hat Enterprise Virtualization template from a guest that was converted by virt-v2v. Guests imported with this updated package can now be used to create templates.

BZ#679017

When converting a 64-bit Windows XP guest to run on Red Hat Enterprise Virtualization, virt-v2v incorrectly identified the guest as 64-bit Windows 2003. 64-bit Windows XP guests are now correctly identified as Windows XP when imported into Red Hat Enterprise Virtualization.

BZ#690286

augeas was not thread safe, and could leak file descriptors when multiple programs attempted to use the libvirt library simultaneously. This resulted in the failure of the calling program. augeas has been modified to remove the global variable that caused this threading issue.

BZ#620449

Sparse storage was not retained across conversion. Storage type is now retained across conversion, but can be modified with the **-oa** flag.

BZ#654531

virt-v2v used enum integers to populate the **ovf:disk-interface** field when converting for Red Hat Enterprise Virtualization. However, this produced an **ovf** file that was not intelligible to Red Hat Enterprise Virtualization Manager. The disk-interface is now populated with correct enum values (**IDE**, **SCSI**, or **VirtIO**), allowing Red Hat Enterprise Virtualization Manager to understand the ovf file.

BZ#664942

When converting a guest to run on Red Hat Enterprise Virtualization, virt-v2v identified created storage as **sparse** or **raw**. This combination is not supported when importing into a data center that uses block storage (fibre channel or iSCSI). virt-v2v can now convert storage format and allocation policy correctly. Additionally, customers can specify a format and allocation policy compatible with the target data center type by using the **-of** and **-oa** command line options.

BZ#671083

virt-v2v conversion would hang if its output was redirected at the command line. This bug was reported and corrected during development. It was not seen in production systems in the field.

BZ#678950

Conversion of a Red Hat Enterprise Linux Desktop virtual machine failed with the following error:

```
Can't locate object method "can_handle" via package
```

```
"Sys::VirtV2V::Converter::RedHat" at
/usr/share/perl5/vendor_perl/Sys/VirtV2V/Converter.pm line 121.
```

This issue has been resolved and conversion should now complete successfully

Enhancements

BZ#581108

virt-v2v can now convert guests which use the qcow2 disk format.

BZ#615977

virt-v2v can now convert Microsoft Windows guests to run on a libvirt or Red Hat Enterprise Virtualization target without requiring the Guest Tools ISO.

BZ#671353

virt-v2v includes support for Windows XP guests with the latest version of virtio-win. New installations of Red Hat Enterprise Linux 6.1 will have this support automatically. Users upgrading from an earlier version of virt-v2v may need to manually alter **/etc/virt-v2v.conf**. If you see the following error message when attempting to convert a Windows XP guest:

```
virt-v2v: No app in config matches os='windows' name='virtio' major='5'
minor='1' arch='i386'
```

the following section must be added to **/etc/virt-v2v.conf**:

```
<app os='windows' major='5' minor='1' arch='i386' name='virtio'>
    <path>/usr/share/virtio-win/drivers/i386/WinXP</path>
  </app>
  <app os='windows' major='5' minor='1' arch='x86_64' name='virtio'>
    <path>/usr/share/virtio-win/drivers/amd64/WinXP</path>
</app>
```

BZ#676553

virt-v2v now enables the conversion of Windows guests which do not have available VirtIO drivers, although these guests are not guaranteed to operate correctly after conversion.

BZ#615182

virt-v2v requires root privileges to convert a guest to run on Red Hat Enterprise Virtualization. When run without these privileges, virt-v2v output an error to this effect but did not fail immediately. This resulted in a number of other error messages being printed, which obscured the primary error. virt-v2v now fails immediately after it outputs the primary privilege error.

BZ#672498

virt-v2v now relies on libvirt to detect volume metadata such as size and format. Guests with volumes that are not contained in a storage pool will therefore fail to be converted. The error message that results from such a failure has been updated to provide detailed information on how to create a storage pool to contain the target volume.

All users of virt-v2v and augeas are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

1.298. virt-viewer

1.298.1. RHEA-2011:0752 — virt-viewer enhancement update

An update to the virt-viewer package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

Virtual Machine Viewer (virt-viewer) is a lightweight interface for interacting with the graphical display of a virtualized guest. It uses libvirt and is intended as a replacement for traditional VNC clients.

Bug Fixes

BZ#651604

The virt-viewer application has been modified to be aware of the new libvirt configuration options for VNC servers, gaining the ability to connect to a VNC server running on a UNIX domain socket.

BZ#631667

When telling virt-viewer to wait for a domain to start (using the -w argument), an error occurred when identifying domains specified based on their UUID, rather than name or ID.

All users requiring virt-viewer should install this new package, which fixes these bugs.

1.299. virtio-win

1.299.1. RHBA-2011:0782 — virtio-win bug fix and enhancement update

Updated virtio-win packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The virtio-win package provides para-virtualized network drivers for most Windows operating systems.

Bug Fixes

BZ#610787

Previously, free eviction memory did not work correctly on Windows guests when using virtio-balloon drivers. This update changes the memory to the set value.

BZ#630536

Previously, the virtual machine aborted unexpectedly when it ran on Windows XP SMP guests. With this update, the guest no longer aborts.

BZ#630830

Previously, the netperf test on the Windows 2008 and Windows 7 guests with virtio network caused the network to become unresponsive. This update corrects the Network Interface Card (NIC) driver. Now, the network stays available.

BZ#633243

Previously, the whql virtio-serial test on Windows 2008 R2 guests caused the subjob "Run SimpleIOStress" to become unresponsive. This update resolves this issue. Now, this subjob runs as expected.

BZ#634828

Previously, the hal.dll file was missing after quitting the Windows XP guest several times. Due to this issue, Windows did not start. This update resolves this issue. The Windows XP guest starts as expected.

BZ#649773

Previously, Windows approved drivers caused an incorrect warning when installing them on Windows 7 x86. This update rebuilds the driver package and CAT file using INF2CAT.

BZ#669314

Previously, virtio-win did not generate crash dump files after encountering a Stop Error (BSOD) of Windows guests. The subjob "Execute Commond_Scenario_Stress_With _IO Script" was aborted. With this update, the subjob passes without further errors.

BZ#669597

Previously, the virtio block driver failed to upgrade and aborted with a BSOD. This update resolves this issue. Now, the virtio block driver upgrades as expected.

BZ#669633

Previously, the job "DPWDK-HotReplace-Device Test-Verify driver support for D3 power state" failed with a BSOD. This update runs this update successfully.

BZ#670713

Previously, the virtio serial driver caused a BSOD when installing or running whql jobs. This update installs the driver and passes all related whql jobs.

BZ#679344

Previously, the viostor.sys file version was not updated between builds. Due to this issue, the RHEV-Block installer could not update this .sys file. This update resolves this issue. Now, the viostor.sys file is updated as expected.

BZ#688839

Previously, windows guests with 30 virtio serial ports aborted booting with a BSOD. With this update, windows guests can boot as expected.

BZ#690713

Previously, the virtio block job "Embedded Signature Verification" failed. This update passes this verification without further errors.

Enhancement

BZ#617000

Previously, the virtio-serial windows driver had a write-size limitation. This limitation caused specific changes to devices using virtio-serial ports in qemu. With this update, write-size is unlimited.

All virtio-win users are advised to upgrade to these updated packages which fix these bugs and add this enhancement.

1.299.2. RHBA-2011:1542 — virtio-win bug fix update

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

The virtio-win package provides paravirtualized network drivers for most Windows operating systems.

The RHBA-2011:0782 virtio-win bug fix and enhancement update did not completely resolve the following issue, which is now fully fixed:

BZ#706791

Previously, the netperf test on the Windows 2008 and Windows 7 guests with virtio network caused the network to become unresponsive. This update corrects the Network Interface Card (NIC) driver. Now, the network stays available.

Bug Fixes

BZ#726883

Previous versions of virtio-win did not include the QXL driver. As a result, the QXL driver could not be installed from the same installation media as the virtio network or block driver. This update adds QXL drivers to the virtio-win installation media. This allows to install and update QXL drivers without requiring the MSI installer.

BZ#728982

The NetKVM driver included in the previous version of virtio-win had a lower version number than the same driver in Red Hat Enterprise Virtualization Manager. It was therefore impossible to update the NetKVM driver when upgrading from Red Hat Enterprise Virtualization 2.2 to 3.0. The most recent NetKVM driver, WHQL (Windows Hardware Quality Labs) signed, takes advantage of the new version numbering scheme, which changed the driver version number to be much higher that before. Users are now able to upgrade the NetKVM driver flawlessly when upgrading from Red Hat Enterprise Virtualization 2.2 to 3.0.

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

1.300. volume_key

1.300.1. RHBA-2011:0298 — volume_key bug fix update

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

The volume_key packages provide a command-line tool and a set of libraries for manipulating storage volume encryption keys and storing them separately from volumes.

The main goal of the software is to allow restoring access to an encrypted hard drive if the primary user forgets the passphrase. The encryption key back up can also be useful for extracting data after a hardware or software failure that corrupts the header of the encrypted volume, or to access the company data after an employee leaves abruptly.

Bug Fixes

BZ#636541

Previously, the volume_key documentation did not specify which of the two block devices to use as an argument to volume_key(8). Due to this problem, unexpected errors caused confusion. With this update, the volume_key.8 man page and the README file clarify whether to use the encrypted or plaintext block device, and how to recognize it.

BZ#638732

Previously, libvolume_key did not provide textual descriptions for a subset of error conditions. Due to this behavior, some error messages contained nonsensical characters instead of readable text. This update adds the missing textual descriptions. The error messages now describe the cause of the error.

BZ#641111

Previously, the volume_key(8) utility could not be interrupted when waiting for a password or passphrase input. This update makes the volume_key(8) utility interruptible in such cases, and notifies the user if the entered passphrase is incorrect.

BZ#643897

Previously, the volume_key(8) utility prompted the user for a passphrase before it validated the supplied certificate file, if any. Due to this behavior, any errors in the file were detected only after the user entered additional information. This update detects and reports such errors immediately, without prompting the user for a passphrase.

All Users are advised to upgrade to these updated volume_key packages, which fix these bugs.

1.301. vte

1.301.1. RHBA-2011:0317 — vte bug fix update

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

VTE is a terminal emulator widget for use with GTK+ 2.0.

Bug Fix

BZ#650884

Due to an error in VTE, using the Shift+left-click combination to select a text in a VTE-based application (for example, GNOME Terminal) could fail to copy this selection into the cut buffer. With this update, an upstream patch has been applied to address this issue, and such selection is now copied to the cut buffer as expected.

All users of vte are advised to upgrade to this updated package, which resolves this issue.

1.302. watchdog

1.302.1. RHEA-2011:0684 — watchdog enhancement update

An updated watchdog package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The watchdog package contains a user-space application which can provide updates to a hardware or software watchdog timer via the Linux kernel's watchdog interface.

Enhancement

BZ#657750

With this update, watchdog creates a /etc/watchdog.d/ directory on installation. Scripts placed in this directory are indexed by the watchdog daemon on startup and are used to monitor or repair resources on the system.

Users of watchdog are advised to upgrade to this updated package which adds this enhancement.

1.303. xerces-j2

1.303.1. RHSA-2011:0858 — Moderate: xerces-j2 security update

Updated xerces-j2 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 xerces-j2 packages provide the Apache Xerces2 Java Parser, a high-performance XML parser. A Document Type Definition (DTD) defines the legal syntax (and also which elements can be used) for certain types of files, such as XML files.

Security Fix

CVE-2009-2625

A flaw was found in the way the Apache Xerces2 Java Parser processed the SYSTEM identifier in DTDs. A remote attacker could provide a specially-crafted XML file, which once parsed by an application using the Apache Xerces2 Java Parser, would lead to a denial of service (application hang due to excessive CPU use).

Users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the Apache Xerces2 Java Parser must be restarted for this update to take effect.

1.304. xguest

1.304.1. RHBA-2011:0194 — xguest bug fix update

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

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#667348

Due to an error in an installation scriptlet, an attempt to install the xguest package failed, and the following error message was written to standard error:

```
/usr/sbin/semanage: No such file or directory
```

This update corrects the %pre scriptlet, and the package can now be installed as expected.

All users of xguest are advised to upgrade to this updated package, which resolves this issue.

1.305. xinetd

1.305.1. RHBA-2011:0784 — xinetd bug fix update

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

The xinetd daemon is a secure replacement for inetd, the Internet services daemon. It provides access control for all services based on the address of the remote host and/or on time of access, and can prevent denial of service attacks.

Bug Fixes

BZ#676013

When a binary is built with the "RELRO" flag, the ELF sections are reordered to include internal data sections before program's data sections, and the Global Offset Table (GOT) address section of the resulting ELF file is mapped read-only. This ensures that any attempt to overwrite the GOT entry and gain control over the execution flow of a program fails with an error. Because of this, the xinetd daemon is now compiled with full RELRO by using the "-Wl,-z,relro,-z,now" gcc option.

BZ#678493

When a log file of a xinetd-controlled service exceeded the size limit specified in its configuration file, xinetd terminated unexpectedly with a segmentation fault. With this update, a patch has been applied to address this issue, and the xinetd daemon no longer crashes.

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

1.306. xkeyboard-config

1.306.1. RHEA-2011:1119 — xkeyboard-config enhancement update

An updated xkeyboard-config package that adds an enhancement is now available for Red Hat Enterprise Linux 6.

The xkeyboard-config package contains configuration data used by the X Keyboard Extension (XKB), which allows selection of keyboard layouts when using a graphical interface.

Enhancement

BZ#712116

The new Unicode character U+20B9 (the Rupee symbol) has been added to Indic keyboard layouts.

Users of xkeyboard-config are advised to upgrade to this updated package, which adds this enhancement.

1.307. xmlrpc-c

1.307.1. RHBA-2011:1284 — xmlrpc-c bug fix update

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

The xmlrpc-c packages provide a network protocol to allow a client program to make a simple RPC (remote procedure call) over the Internet. It converts the RPC into an XML document, sends it to a remote server using HTTP, and gets back the response in XML.

Bug Fix

BZ#729793

Prior to this update, the GSSAPI credential delegation was disabled due to a security issue. As a result, the functionality of applications that relied on delegation was broken. This update adds a new constructor argument in the xmlrpc-c++ client API to set the new CURLOPT_GSSAPI_DELEGATION libcurl option to enable the credential delegation. All applications that use xmlrpc-c with GSSAPI credential delegation can now apply this new constructor to run as expected.

Users of xmlrpc-c are advised to upgrade to these updated packages, which fix this bug.

1.308. xorg-x11-drv-intel

1.308.1. RHEA-2011:0618 — xorg-x11-drv-intel enhancement update

Updated xorg-x11-drv-intel packages that add an enhancement are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-intel package contains an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

Enhancement

BZ#667564

The xorg-x11-drv-intel packages now support Sandy Bridge graphics chipsets, as found on second generation Intel Core i7 series processors.

All xorg-x11-drv-intel users should upgrade to these updated packages, which add this enhancement.

1.309. xorg-x11-drv-mga

1.309.1. RHEA-2011:0778 — xorg-x11-drv-mga enhancement update

An updated xorg-x11-drv-mga package that adds various enhancements is now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-mga package is a video driver for Matrox G-series chipsets for the X.Org implementation of the X Window System.

Enhancements

BZ#672813

The xorg-x11-drv-mga package now supports the Matrox MGA-G200ER graphics card found in servers and integrated management consoles.

BZ#660630

The xorg-x11-drv-mga package now supports the Onboard Matrox graphics controller found in Dell PowerEdge servers.

BZ#674556

With this update, the xorg-x11-drv-mga package provides an update to the IMMv2 management controller for the integrated Matrox G200 graphics card series. These devices are now fully compatible with the X Window System in Red Hat Enterprise Linux 6.

All xorg-x11-drv-mga users should upgrade to this updated package, which adds these enhancements.

1.309.2. RHBA-2011:1123 — xorg-x11-drv-mga bug fix update

An updated xorg-x11-drv-mga package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-mga package is a video driver for Matrox G-series chipsets for the X.Org implementation of the X Window System.

BZ#717192

Previously, the MGA driver rendered the image incorrectly on big-endian architectures, including PowerPC and 64-bit PowerPC. Consequently, the display showed altered colors. With this update, a patch has been provided to address this issue, and the colors are now displayed correctly in the described scenario.

All users of xorg-x11-drv-mga are advised to upgrade to this updated package, which fixes this bug.

1.310. xorg-x11-drv-nouveau

1.310.1. RHBA-2011:0594 — xorg-x11-drv-nouveau bug fix update

Updated xorg-x11-drv-nouveau packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-nouveau utility provides the Xorg X11 nouveau video driver for NVIDIA graphics chipsets.

Bug Fix

BZ#633226

Previously, the Xorg X11 nouveau video driver incorrectly tried to access acceleration-related structures for rotation on chipsets with disabled acceleration. Due to this behavior, the driver aborted unexpectedly. Now, rotation works regardless of whether acceleration is enabled or not.

All users of xorg-x11-drv-nouveau are advised to upgrade to these updated packages, which fix this bug.

1.311. xorg-x11-drv-qxl

1.311.1. RHBA-2011:0756 — 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 package includes support for rev. 02 devices with surfaces. (BZ#670009)

Bug Fixes

BZ#623652

When using the qxl driver, resolution choices inside the guest would not exceed 1024x768 in size unless the xorg.conf configuration file was created and manually edited. This update ensures that larger resolutions are now available for guests with appropriate hardware without requiring a manual change to the xorg.conf file.

BZ#626508

When using the qxl driver, when connected to a virtual guest using SPICE and logging into a desktop session from the GDM display manager, switching to a virtual console using a key combination caused a server 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 now works as expected.

BZ#680120

Xorg crashed shortly after X started up. This was caused by an insufficient amount of video memory made available to the qxl device. This update fixes this by making additional memory available to Xorg so that it no longer crashes.

BZ#680865

Running the Xorg command with the configure parameter (Xorg -configure) using the qxl driver resulted in a blacked out console window. This update provides a fix so that Xorg no longer crashed when run with the -configure parameter.

BZ#684994

The description field against the X.Org X11 qxl video driver was non-descriptive and stated only the name of the driver. This is now fixed to include descriptive information about the video driver.

Users are advised to upgrade to this updated xorg-x11-drv-qxl package.

1.312. xorg-x11-drv-wacom

1.312.1. RHEA-2011:0807 — xorg-x11-drv-wacom and wacomcpl enhancement update

Updated xorg-x11-drv-wacom and wacomcpl packages that add one enhancement 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.

Enhancement

BZ#620957

Prior to this update, the "wacom" input driver did not provide support for Wacom Cintiq 21UX2. With this update, the input driver and wacomcpl have been adapted to support the Wacom Cintiq 21UX2 devices.

All users of xorg-x11-drv-wacom and wacomcpl are advised to upgrade to these updated packages, which add this enhancement.

1.313. xorg-x11-drv-xgi

1.313.1. RHBA-2011:0793 — xorg-x11-drv-xgi and xorg-x11-drivers bug fix and enhancement update

A new xorg-x11-drv-xgi package, and an updated xorg-x11-drivers package that fixes a bug and adds an enhancement, are now available for Red Hat Enterprise Linux 6.

The new xorg-x11-drv-xgi package contains a video driver for XGI Z-series graphics chips for the X.Org implementation of the X Window System.

The xorg-x11-drivers package contains all of the individual X.Org drivers, to allow installation of all drivers at once, without having to track which individual drivers are present on each architecture.

This enhancement update adds the xorg-x11-drv-xgi package to Red Hat Enterprise Linux 6. The xorg-x11-drv-xgi package has been introduced to provide support for XGI Z7, Z9, and Z11 series chips. This new package adds native support for these chips, including native video mode setup, 2D acceleration, and hardware cursor support. (BZ#683979)

Bug Fix

BZ#693652

Previously, the X Window System failed to load a module containing a driver for the XGI graphics cards. This bug has been fixed and the module is now properly loaded when generating an xorg.conf configuration file.

Enhancement

BZ#526038, BZ#631738

The driver for XGI Volari Z9s graphics cards has been updated for newer server system support.

All users of XGI graphics cards should install this new package, and upgrade these updated packages, which fix this bug and add this enhancement.

1.313.2. RHBA-2011:1415 — xorg-x11-drv-xgi bug fix update

An updated xorg-x11-drv-xgi package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-xgi package provides a video driver for XGI Z-series graphics chips for the X.Org implementation of the X Window System.

Bug Fix

BZ#730649

Due to a missing XGIPowerSaving() function call in the xgi video driver's source code, a server using XGI Z9-series graphics chipset was not able to recover from power-saving mode. With this update, the XGIPowerSaving() function call has been added and the server now recovers properly.

All users of xorg-x11-drv-xgi are advised to upgrade to this updated package, which fixes this bug.

1.314. xorg-x11-server

1.314.1. RHSA-2011:1359 — Moderate: xorg-x11-server security update

Updated xorg-x11-server packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Security Fixes

CVE-2010-4818

Multiple input sanitization flaws were found in the X.Org GLX (OpenGL extension to the X Window System) extension. A malicious, authorized client could use these flaws to crash the X.Org server or, potentially, execute arbitrary code with root privileges.

CVE-2010-4819

An input sanitization flaw was found in the X.Org Render extension. A malicious, authorized client could use this flaw to leak arbitrary memory from the X.Org server process, or possibly crash the X.Org server.

Users of xorg-x11-server should upgrade to these updated packages, which contain backported patches to resolve these issues. All running X.Org server instances must be restarted for this update to take effect.

1.314.2. RHBA-2011:0543 — xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix one bug are now available.

The xorg-x11-server provides the X.Org sample implementation of a server for the X Window System. It provides the rendering services necessary for graphical user environments like GNOME.

Bug Fix

BZ#625564, BZ#627719, BZ#633281, BZ#636904, BZ#638234

In previous releases, drivers using RANDR-style output setup (Radeon, Nouveau, and Intel) selected a default resolution of 1024x768 when no EDID information was available from the monitor. Older, non-RANDR-style drivers, however,defaulted to 800x600 in this situation. This update corrects the defaults for non-RANDR-style drivers to 1024x768 for consistency.

All xorg-x11-server users are advised to upgrade to these updated packages, which fix this bug.

1.315. yaboot

1.315.1. RHBA-2011:1475 — yaboot bug fix update

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

The yaboot package provides a boot loader for Open Firmware based PowerPC systems. The Yaboot boot loader can be used to boot IBM System p machines.

Bug Fix

BZ#747716

The Yaboot boot loader did not store additional arguments that were provided by a user on system boot, therefore these arguments were discarded whenever the Client Architecture Support (CAS) firmware interface initialized system reboot. This behavior prevented, under certain circumstances, the Anaconda installer from proper system installation. Yaboot has been modified to keep additional boot parameters, and the parameters required for proper system installation are now passed to Anaconda as expected.

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

1.316. yum

1.316.1. RHBA-2011:0602 — yum bug fix and enhancement update

Updated yum packages that fix number of bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The yum package has been upgraded to upstream version 3.2.29, which provides a number of bug fixes and enhancements over the previous version. (BZ#659494)

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#628151

Previously, yum treated packages that provide kernel modules as install-only packages. With this update, the install-only option has been removed.

BZ#632391

Previously, yum didn't properly delete .sqlite files it generated. This caused the /var/cache/yum/ directory to fill up with new unique sqlite files every day, even if users didn't perform any yum request or commands. Now, yum cleans these generated files as expected.

BZ#700035

After manually clearing the yum cache by removing all files under the /var/cache/yum/ directory, running the "yum update" or "yum clean all" commands could have resulted in failure with the following error message:

```
There are no enabled repos.
```

With this update, yum proceeds as expected with downloading repodata even after manually clearing the cache.

BZ#607258

Running the "yum localinstall" command with a delta RPM file as an argument caused yum to terminate with a traceback. With this update, a more specific error message is displayed instead of the traceback.

BZ#633270

When yum tried to retrieve repository data from a channel with SHA-384 checksum, yum terminated. With this update, support for SHA-384 checksums has been added and yum can access such channels properly.

BZ#663378

Running "yum --changelog update" caused yum to terminate with a traceback. With this update, an informative error message is given instead.

BZ#679760

On the i686 platform, if a user tried to install a package bigger than 2 GB, yum terminated. With this update, support for such packages has been added.

BZ#604973

When a yum repository ID contained a yum variable such as "$basearch", enabling or disabling that repository using the PackageKit GUI caused yum to fail with a traceback. This update ensures that yum variables in repository IDs are handled properly, and yum no longer fails in this scenario.

BZ#623553

When yum was given two arguments to reinstall the same package, it redundantly removed and reinstalled the package twice. With this update, a package is only removed once before reinstallation if multiple arguments are passed to yum.

BZ#630983

When a version lock was specified for a particular version of a package that was also obsoleted by a newer package, the newer package was not properly updated when "yum update" was called and yum exited with an error message. This bug has been fixed and updates of such packages are now performed as expected and no error messages are given.

BZ#634595

Previously, when concurrent yum and RPM transactions were running, yum sometimes terminated with a traceback. With this update, transaction conflicts are properly recognised, and when they are encountered, yum exits with a proper error message.

BZ#669746

When a non-root user ran yum using the "--cacheonly" ("-C") option, yum terminated with a traceback. With this update, yum provides a proper error message in this circumstance.

BZ#677410

Certain commits caused yum to hold the RPM database open throughout the remaining package download, after the first signature check happened. As a consequence, when a user pressed Ctrl+C, the shortcut could not be properly recognized and reacted upon. With this update, this bug has been fixed and no longer occurs.

BZ#678043

When yum called the pkgSack.searchNevra() function to get information about a package, the call

failed and the "Unable to fetch [package] package" error was given, while "yum install [package]" command worked correctly. With this update, this bug has been fixed and the error message is no longer given if the package in question is available.

BZ#683946

After having installed a 64-bit package and running "yum localupdate" command with the same package for both 64-bit and 32-bit architectures, yum installed the 32-bit package if the file list contained the current package versions. This bug has been fixed and yum now checks for installed packages and does nothing in the described scenario.

BZ#692866

When running "yum --version" command, yum displayed the following redundant lines to the output:

```
INFO:rhsm-app.repolib:repos updated:
Ignored option -q, -v, -d or -e (probably due to merging: -yq != -y -q)
```

With this update, this bug has been fixed and the redundant lines are no longer displayed.

BZ#695427

Previously, users were not notified that different certificate files with the same basename are treated as identical, which could lead to all sorts of problems. With this update, yum checks certificate files for such duplicates and displays an error message appropriately.

BZ#696720

When a package was reinstalled, yum generated RPM database entries that included both the old and new versions of the package, leading to various issues. This bug has been fixed and now only correct RPM database entries are generated for reinstalled packages.

BZ#655281

Previously, when the "yum groupinstall" command was called to install a package with a dependency that had not been met, the package was not in fact installed but the user was not informed about the situation properly. This bug has been fixed and yum now prints a warning if a package cannot be installed due to a missing requirement.

Enhancements

BZ#602149

This update extends yum functionality by adding yum-cron package. It provides automatic background system updates with no user intervention and replaces the outdated yum-updatesd package.

BZ#606644

Previously, when import of a second GPG key was not allowed during the installation of a package, yum exited even if import of the first GPG key was successful. With this update, the transaction will continue as long as at least one GPG key was successfully imported.

BZ#634117

With this update, yum is able to parse advisory detail metadata stored in updateinfo.xml files provided by each channel in Red Hat Network. This enhancement allows more information to be provided to customers via GUI and CLI tools including things such as errata severity.

BZ#652750

With this update, in output of the "yum grouplist" command, software groups and language groups are separated and sorted independently, making the whole list much clearer to read. Additionally, a language code is appended to each entry in the language group list.

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

1.316.2. RHBA-2011:1403 — yum bug fix update

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

Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically, prompting a user for permission as necessary.

Bug Fix

BZ#744150

Previously, the Pulp application used the RepoStorage API directly outside of the YumBase class, therefore certain attributes were not set as expected. As a consequence, users experienced attributes errors when using the Pulp server to manage their software repositories. With this update, RepoStorage has been modified to include the condition that verifies and sets these attributes. These attributes errors occur no more when using Pulp.

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

1.317. yum-metadata-parser

1.317.1. RHBA-2011:0781 — yum-metadata-parser bug fix update

An updated yum-metadata-parser package that fixes a bug is now available for Red Hat Enterprise Linux 6.

The yum-metadata-parser package provides a fast metadata parser for Yum implemented in C.

Bug Fix

BZ#612409

Due to an error in the conversion of SQLite data for large packages, an attempt to install a package larger than 2GB caused Yum to incorrectly represent the package size as a negative number. This update ensures that yum-metadata-parser converts all data to SQLite correctly, and package sizes are now always represented as expected.

All users should upgrade to this updated package, which resolves this issue.

1.318. yum-rhn-plugin

1.318.1. RHBA-2011:0516 — yum-rhn-plugin bug fix update

An updated yum-rhn-plugin package which fixes a bug is now available for Red Hat Enterprise Linux 6.

Yum-rhn-plugin allows yum to access a Red Hat Network server for software updates.

Bug Fix

BZ#703586

When used in conjunction with yum 3.2.29, yum-rhn-plugin created empty and superfluous directories for every registered RHN repository in the current directory when "yum clean" was executed. Note: directories for other registered yum repositories were not created in this instance. With this update, no directories are created when "yum clean" is executed, as expected.

Yum-rhn-plugin users are advised to upgrade to this updated package, which resolves this issue.

1.319. yum-utils

1.319.1. RHBA-2011:0603 — yum-utils bug fix and enhancement update

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

The yum-utils packages contain a collection of utilities and examples for the yum package manager. They include utilities by different authors that make yum easier and more powerful to use.

Bug Fixes

BZ#674584

Previously, the yum-plugin-aliases package could not be installed or imported due to a minor bug in the code. With this update, the bug has been fixed and the plug-in can now be properly installed and imported.

BZ#679098

When a yum repository ID contained a yum variable such as "$basearch", enabling or disabling that repository using the yum-config-manager utility caused yum to fail with a traceback. This update ensures that yum variables in repository IDs are handled properly, and yum no longer fails in this scenario.

BZ#604529

Previously, the yum-plugin-verify utility recognized very short change times in packages. As a consequence, packages were reported for changes in mtime shorter than one second. This bug has been fixed and the yum-plugin-verify utility no longer reports such short change times.

BZ#616408

The "--archlist" option of the yumdownloader utility was not properly documented in the yum-utils manual page. With this update, the missing part of the documentation has been added.

BZ#620652

Previously, when the repomanage utility was called with a non-existent directory as one of its arguments, it terminated with a traceback. This bug has been fixed and a proper error message is displayed in this scenario.

BZ#627533

Previously, the tsflags plug-in used a deprecated API, resulting in unnecessary output messages when the plug-in was used. This bug has been fixed and no redundant messages are now displayed.

BZ#641837

When options were passed to yum-debug-dump utility, the options were incorrectly parsed as additional arguments. As a consequence, the yum-debug-dump utility sometimes saved its output to the wrong file. With this update, options and arguments are properly parsed by the yum-debug-dump utility and this bug no longer occurs.

Enhancements

BZ#662790

With this update, the security plug-in is able to parse advisory detail metadata stored in updateinfo.xml files provided by each channel in Red Hat Network. This enhancement allows more information to be provided to customers via GUI and command line programs, including details such as errata severity.

BZ#669178

Previously, error messages of the yum-plugin-fs-snapshot plug-in were unnecessarily complicated and long, which made them hard to read. With this update, the error messages have been updated to provide a better overview when a problem occurs with the plug-in.

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

2. NEW PACKAGES

2.1. RHEA-2011:0533 — new package: 389-ds-base

New 389-ds-base packages are now available for Red Hat Enterprise Linux 6.

The 389 Directory Server is an LDAPv3 compliant server.

The 389-ds-base package includes the LDAP server and command line utilities for server administration.

This enhancement update adds the 389-ds-base package to Red Hat Enterprise Linux 6. (BZ#642408)

All users who require the 389 Directory Server are advised to install these new packages.

2.2. RHEA-2011:0664 — new package: PyPAM

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

PyPAM is a Python module that provides an interface to the pluggable authentication modules (PAM). These bindings allow Python applications to authorize, authenticate, and manage user sessions through the system's PAM configuration.

This enhancement update adds the PyPAM package to Red Hat Enterprise Linux 6. (BZ#667127)

All users requiring PyPAM should install this newly-released package, which adds this enhancement.

2.3. RHEA-2011:0644 — new package: biosdevname

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

Traditionally, network interfaces in Linux are named eth[X]. However, in many cases, these names do not correspond to actual labels on the chassis. Modern server platforms with multiple network adapters can encounter non-deterministic and counter-intuitive naming of these network interfaces.

This update for Red Hat Enterprise Linux 6 introduces biosdevname, an optional convention for naming network interfaces. biosdevname assigns names to network interfaces based on their physical location.

Note that biosdevname is disabled by default, except for a limited set of Dell PowerEdge, C Series and Precision Workstation systems.

Further information on the new biosdevname feature is available in this Knowledgebase article.

2.4. RHEA-2011:0589 — new package: compat-openldap

A new compat-openldap package is now available for Red Hat Enterprise Linux 6.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. The compat-openldap package provides compatibility libraries for the OpenLDAP suite.

Previously, the compat-openldap package was released as a subpackage of openldap. This enhancement update adds compat-openldap to Red Hat Enterprise Linux 6 as a separate package. (BZ#652309)

All users who require compat-openldap should install this new package.

2.5. RHEA-2011:0562 — new package: ding-libs

New ding-libs packages are now available for Red Hat Enterprise Linux 6.

Ding-libs is a set of helpful libraries used by SSSD and other projects.

Ding-libs provides utility functions to manipulate filesystem pathnames (libpath_utils), a hash table which dynamically resizes to achieve optimal storage and access time properties (libdhash), a data type to collect data in a hierarchical structure for easy iteration and serialization (libcollection), a dynamically growing, reference-counted array (libref_array), and a library to process configuration files in initialization format (INI) into a library collection data structure (libini_config).

This enhancement update adds the ding-libs packages to Red Hat Enterprise Linux 6. (BZ#644073)

All users requiring ding-libs are advised to install these new packages.

2.6. RHEA-2011:0635 — new package: foghorn

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

The foghorn daemon listens for specific signals on the D-Bus message bus system and translates these signals into SNMP traps.

This enhancement update adds the foghorn package to Red Hat Enterprise Linux 6. (BZ#660324)

All users who require foghorn should install this new package.

2.7. RHEA-2011:0579 — new package: hwloc

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

The hwloc package provides Portable Hardware Locality, which is a portable abstraction of the hierarchical topology of current architectures.

This enhancement update adds the hwloc package to Red Hat Enterprise Linux 6. (BZ#648593)

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

2.8. RHEA-2011:0658 — new package: icedtea-web

New icedtea-web packages are now available for Red Hat Enterprise Linux 6.

The IcedTea-Web project provides a Java web browser plug-in and an implementation of Java Web Start, which is based on the NetX project. It also contains a preview version of a configuration tool for managing deployment settings for the plug-in and Web Start implementations.

This enhancement update adds the icedtea-web packages to Red Hat Enterprise Linux 6. (BZ#664063)

All users who require icedtea-web are advised to install these new packages.

2.9. RHEA-2011:0631 — new package: ipa

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

Red Hat Enterprise Identity (IPA) is a centralized authentication, identity management and authorization solution for both traditional and cloud based enterprise environments. It integrates components of the Red Hat Directory Server, MIT Kerberos, Red Hat Certificate System, NTP and DNS. It provides web browser and command-line interfaces. Its administration tools allow an administrator to quickly install, set up, and administer a group of IPA servers to meet the authentication and identity management requirements of the large scale Linux and Unix deployments.

This enhancement update adds new ipa packages to Red Hat Enterprise Linux 6. (BZ#658275)

All users requiring ipa should install these newly-released packages, which add these enhancements.

2.10. RHEA-2011:0624 — new package: ipa-pki-theme

A new ipa-pki-theme package is now available for Red Hat Enterprise Linux 6.

ipa-pki-theme provides IPA theme components for PKI packages.

The Certificate System (CS) manages enterprise Public Key Infrastructure (PKI) deployments and requires a theme for the specific type of PKI deployment with which it is used. Previously, no PKI theme existed for Identity, Policy, Audit (IPA) deployments on Red Hat Enterprise Linux 6. This new package makes an IPA theme available for CS, and therefore makes it possible for users of Red Hat Enterprise Linux 6 to use CS to manage IPA deployments.

Important -- this theme is mutually exclusive with the PKI themes for other types of PKI deployments, such as dogtag-pki-theme for Dogtag Certificate System deployments and redhat-pki-theme for Red Hat Certificate System deployments. (BZ#643543)

Users who want to use CS to manage IPA deployments are advised to install this new package.

2.11. RHEA-2011:0811 — new package: iwl100-firmware

A new iwl100-firmware package is now available.

This package contains the firmware required by the iwlagn driver for Linux to support the iwl100 hardware.

The firmware for the Crane Peak 1(100) Wifi network adaptor was not included with its driver (iwlagn) in the earlier release. This is now included with the driver in RHEL6.1. (BZ#694078)

All users requiring iwlagn should install this new package, which adds this enhancement.

2.12. RHEA-2011:0552 — new package: iwl6000g2a-firmware

A new iwl6000g2a-firmware package that works with the iwlagn driver in the latest Red Hat Enterprise Linux kernels to enable support for Intel Wireless WiFi Link 6005 Series AGN Adapters is now available.

iwlagn is a kernel driver module for the Intel Wireless WiFi Link series of devices. The iwlagn driver requires firmware loaded on the device in order to function.

This new iwl6000g2a-firmware package provides the firmware required by iwlagn to enable Intel Wireless WiFi Link 6005 Series AGN Adapters. (BZ#663971)

All users of the iwlagn driver, especially those requiring iwl6000g2a support, should install this new package, which provides this enhancement.

2.13. RHEA-2011:0553 — new package: iwl6000g2b-firmware

A new iwl6000g2b-firmware package that works with the iwlagn driver in the latest Red Hat Enterprise Linux kernels to enable support for Intel Wireless WiFi Link 6030 Series AGN Adapters is now available.

iwlagn is a kernel driver module for the Intel Wireless WiFi Link series of devices. The iwlagn driver requires firmware loaded on the device in order to function.

This new iwl6000g2b-firmware package provides the firmware required by iwlagn to enable Intel Wireless WiFi Link 6030 Series AGN Adapters. (BZ#664520)

All users of the iwlagn driver, especially those requiring iwl6000g2b support, should install this new package, which provides this enhancement.

2.14. RHEA-2011:0660 — new package: kdewebdev

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

KDEWebdev provides a set of KDE-based programmers' utilities for web development.

KDEWebdev provides a web-based integrated development environment (Web IDE), a stylesheet debugger, and a utility to search and replace strings. (BZ#591964)

All users who wish to use the KDE-based set of web applications are advised to install this new package.

2.15. RHEA-2011:0777 — new package: libcxgb4

New libcxgb4 packages are available for Red Hat Enterprise Linux 6.

libcxgb4 provides a userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio Internet Wide Area RDMA Protocol (iWARP) capable ethernet devices.

This enhancement update adds the libcxgb4 package to Red Hat Enterprise Linux 6. (BZ#675024)

All users of Chelsio iWARP capable ethernet devices are advised to install these new packages.

2.16. RHEA-2011:0656 — new package: libnes

The libnes package is now available.

libnes is a userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables NetEffect iWARP capable ethernet devices.

This update adds the libnes driver to the distribution. (BZ#664801)

All users requiring libnes should install this new package, which adds this enhancement.

2.17. RHEA-2011:0669 — new package: matahari

New matahari packages are now available for Red Hat Enterprise Linux 6. A new mingw32-matahari package, which accompanies matahari, is also now available for Red Hat Enterprise Linux 6.

The matahari packages provide a set of APIs for operating system management that are exposed for remote access over the Qpid Management Framework (QMF).

The mingw32-matahari package provides the Windows variant of matahari, compiled with the mingw32 compiler toolchain.

This enhancement update adds new matahari and mingw32-matahari packages to Red Hat Enterprise Linux 6. (BZ#658828, BZ#658840)

All users requiring matahari and mingw32-matahari should install these newly-released packages, which add these enhancements.

2.18. RHEA-2011:0629 — new package: mod_revocator

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

The mod_revocator module retrieves and installs remote Certificate Revocation Lists (CRLs) into an Apache web server without a need for a restart or user intervention. It can be configured to retrieve CRLs from remote servers at periodic intervals or when a CRL expires, and make them available to the Apache Secure Sockets Layer (SSL) module, mod_nss. Additionally, it can be configured to stop the Apache HTTP Server from accepting requests if a CRL retrieval fails.

This enhancement update adds the mod_revocator package to Red Hat Enterprise Linux 6. (BZ#584103)

All users who require mod_revocator should install this new package.

2.19. RHEA-2011:0625 — new package: netxen-firmware

A new netxen-firmware package is now available.

netxen_nic is a kernel driver module for the QLogic netxen P3 devices. It works with the netxen_nic driver in the latest Red Hat Enterprise Linux kernels to enable support for QLogic Intelligent Ethernet (3000 and 3100 Series) netxen P3 adapters.

This new netxen-firmware package provides the firmware required by netxen_nic to enable QLogic Linux Intelligent Ethernet (3000 and 3100 Series) Adapter. (BZ#562940)

All users of the netxen_nic driver should install this new package, which provides this enhancement.

2.20. RHEA-2011:0572 — new package: nuxwdog

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

The nuxwdog packages provide a watchdog daemon that is used to start, stop, and monitor system processes, as well as to prompt users for passwords when required. Additionally, interfaces to the client code for various programming languages are included to allow clients to interact with the nuxwdog daemon.

This enhancement update adds the nuxwdog packages to Red Hat Enterprise Linux 6. (BZ#643546)

All users who require nuxwdog should install these new packages.

2.21. RHEA-2011:0528 — new package: omping

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

Open Multicast Ping (omping) is a tool for testing IP multicast functionality, primarily on a LAN (local area network). It allows users to test multicast and receive sufficient information to detect whether a potential problem exists in the network configuration, or lies elsewhere, as might be the case with a bug.

This enhancement update adds a new omping package to Red Hat Enterprise Linux 6 as a Technology Preview. (BZ#657370)

More information about Red Hat Technology Previews is available here:

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

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

2.22. RHEA-2011:0626 — new package: osutil

A new osutil package is now available.

The Operating System Utilities Java Native Interface (JNI) package supplies various native operating system operations to Java programs.

This new package adds JNI features that allow Red Hat Enterprise Linux 6 users to use the operating system utility libraries that are made available to java programs using JNI. Red Hat IPA and the Certificate System CA depend on JNI for their interface with the operating system. (BZ#643543)

Users are advised to upgrade to this updated package, which resolves this issue.

2.23. RHEA-2011:0623 — new package: perl-Class-MethodMaker

A new perl-Class-MethodMaker package is now available for Red Hat Enterprise Linux 6.

Class::MethodMaker is a Perl module that enables the creation of generic methods. This makes it easier to write accessor methods for objects that perform standard tasks.

This enhancement update adds the perl-Class-MethodMaker package to Red Hat Enterprise Linux 6. (BZ#669046)

All users who require the Class::MethodMaker Perl module should install this new package.

2.24. RHEA-2011:0709 — new package: perl-IO-Tty

A new perl-IO-Tty package is now available for Red Hat Enterprise Linux 6.

The perl-IO-Tty package provides the IO::Tty and IO::Pty Perl modules that allow for the creation of a pseudo-tty (Berkeley Unix networking device). This package allows to determine the correct terminal width even for terminals with less than 50 columns.

This new package adds the IO::Tty and IO::Pty Perl modules to Red Hat Enterprise Linux 6. (BZ#669405)

All users of pseudo-tty devises are advised to install this new package.

2.25. RHEA-2011:0723 — new package: perl-IPC-Run

A new perl-IPC-Run package is now available for Red Hat Enterprise Linux 6.

The IPC::Run module provides a mechanism for Perl scripts to interact with child processes.

This enhancement update adds the perl-IPC-Run package to Red Hat Enterprise Linux 6. (BZ#669403)

All users who require the IPC::Run Perl module should install this new package.

2.26. RHEA-2011:0617 — new package: perl-Parse-RecDescent

A new perl-Parse-RecDescent package is now available for Red Hat Enterprise Linux 6.

The Parse::RecDescent module provides a mechanism for Perl scripts to generate top-down recursive-descent text parsers from grammar specifications similar to yacc.

This enhancement update adds the perl-Parse-RecDescent package to Red Hat Enterprise Linux 6. (BZ#643547)

All users who require the Parse::RecDescent Perl module should install this new package.

2.27. RHEA-2011:0640 — new package: perl-Term-ProgressBar

A new perl-Term-ProgressBar package is now available for Red Hat Enterprise Linux 6.

The Term::ProgressBar module provides a mechanism for Perl scripts to display a progress bar on the command line.

This enhancement update adds the perl-Term-ProgressBar package to Red Hat Enterprise Linux 6. (BZ#665417)

All users who require the Term::ProgressBar Perl module should install this new package.

2.28. RHEA-2011:0605 — new package: perl-TermReadKey

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

The Term::ReadKey module provides a mechanism for Perl scripts to control various terminal driver modes, perform non-blocking reads, and interact with a terminal.

This enhancement update adds the perl-TermReadKey package to Red Hat Enterprise Linux 6. (BZ#665415)

All users who require the Term::ReadKey Perl module should install this new package.

2.29. RHEA-2011:0627 — new package: pki-core

New pki-core packages are now available for Red Hat Enterprise Linux 6.

Red Hat Certificate System is an enterprise software system designed to manage enterprise public key infrastructure (PKI) deployments. PKI Core contains fundamental packages required by Red Hat Certificate System, which comprise the Certificate Authority (CA) subsystem.

Note: The Certificate Authority component provided by this errata cannot be used as a standalone server. It is installed and operates as a part of the Red Hat Enterprise Identity (IPA).

This enhancement update adds the pki-core packages to Red Hat Enterprise Linux 6. (BZ#645097)

All users should install these new packages.

2.30. RHEA-2011:0612 — new package: python-kerberos

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

This new python-kerberos package contains a high-level wrapper for Kerberos (GSSAPI) operations.

This limited set provides all needed functions for client-server Kerberos authentication. (BZ#601111)

Users who require Kerberos authentication for or from Python programs are advised to install this new python-kerberos package.

2.31. RHEA-2011:0613 — new package: python-krbV

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

Kerberos is a network authentication system. The krbV module provides a Python binding to the Kerberos 5 libraries, and allows Python programs to utilize Kerberos functions and services.

This enhancement update adds the python-krbV package to Red Hat Enterprise Linux 6. (BZ#642414)

All users who require the krbV Python module should install this new package.

2.32. RHEA-2011:0622 — new package: python-netaddr

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

The python-netaddr package provides a network address representation and manipulation library for Python. The netaddr library allows Python applications to work with IPv4 and IPv6 addresses, subnetworks, non-aligned IP address ranges and sets, MAC addresses, Organizationally Unique

Identifiers (OUI), Individual Address Blocks (IAB), and IEEE EUI-64 identifiers.

This enhancement update adds the python-netaddr package to Red Hat Enterprise Linux 6. (BZ#658557)

All users who require python-netaddr should install this new package.

2.33. RHEA-2011:0630 — new package: python-pyasn1

A new python-pyasn1 package is now available for Red Hat Enterprise Linux 6.

The python-pyasn1 package provides an implementation of ASN.1 types (concrete syntax) and codecs (transfer syntax) for the Python programming language.

This enhancement update adds the python-pyasn1 package to Red Hat Enterprise Linux 6. (BZ#643555)

All users who require python-pyasn1 should install this new package.

2.34. RHEA-2011:0608 — new package: python-rhsm

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

The new python-rhsm package provides access to the Subscription Management tools. It helps users to understand specific products which are installed on their machines and specific subscriptions which their machines consume.

This enhancement update adds a new python-rhsm package to Red Hat Enterprise Linux 6. (BZ#661863)

All users requiring python-rhsm should install this newly-released package, which adds this enhancement.

2.35. RHEA-2011:0805 — new package: qpid-qmf

New qpid-qmf packages are now available for Red Hat Enterprise Linux 6.

The qpid-qmf package provides an extensible management framework layered on QPID messaging.

This enhancement update adds the qpid-qmf package. The qpid-qmf package is now the top-level package for various QMF components which were previously packaged in their own RPM packages (specifically, the python-qmf and qpid-cpp packages). (BZ#691836)

All users who require qpid-qmf should install this new package.

2.36. RHEA-2011:0654 — new package: ras-utils

A new ras-utils package is now available for Red Hat Enterprise Linux 6.

The ras-utils package contains both the aer-inject (for PCIE AER Injection) and mce-inject (MCE Injection) tools. These tools can be used to insert software-simulated AER and MCE errors.

This enhancement update adds a new ras-utils package to Red Hat Enterprise Linux 6. (BZ#653481)

All users requiring ras-utils should install these newly-released package, which adds this enhancement.

2.37. RHEA-2011:0691 — new package: ruby-shadow

A new ruby-shadow package is now available for Red Hat Enterprise Linux 6.

The ruby-shadow package provides Ruby bindings for shadow password access.

This enhancement update adds the ruby-shadow package to Red Hat Enterprise Linux 6. (BZ#658521)

Users who require Ruby bindings for shadow password access are advised to install this new package.

2.38. RHEA-2011:0671 — new package: scons

New scons packages as well as new mingw32-* packages, which provide dependencies for building the Matahari agents for Windows guests, are now available for Red Hat Enterprise Linux 6.

Matahari is a set of APIs for operating system management that are exposed for remote access over the Qpid Management Framework (QMF).

This enhancement update adds new scons and mingw32 dependency packages to Red Hat Enterprise Linux 6 as a Technology Preview. These packages provide the mingw32 compiler dependencies needed to cross-compile Matahari agents for Windows. (BZ#658833)

More information about Red Hat Technology Previews is available here:

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

The complete list of packages provided by this update is as follows:

* scons

* mingw32-binutils

* mingw32-boost

* mingw32-bzip2

* mingw32-dlfcn

* mingw32-expat

* mingw32-filesystem

* mingw32-gcc

* mingw32-gettext

* mingw32-glib2

* mingw32-gnutls

* mingw32-iconv

* mingw32-libgcrypt

* mingw32-libgpg-error

* mingw32-libxml2

* mingw32-libxslt

* mingw32-nsis

* mingw32-pcre

* mingw32-pthreads

* mingw32-qpid-cpp

* mingw32-readline

* mingw32-runtime

* mingw32-sigar

* mingw32-srvany

* mingw32-termcap

* mingw32-w32api

* mingw32-zlib

All users who need to cross-compile Matahari agents for Windows should install these packages, which provide this enhancement.

2.39. RHEA-2011:0670 — new package: sigar

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

The System Information Gatherer and Reporter (SIGAR) is a library and command line tool for accessing operating system and hardware level information across multiple platforms and programming languages.

This enhancement update adds the sigar package to Red Hat Enterprise Linux 6. Note that this package is included as a Technology Preview. (BZ#658887)

All users who require sigar should install this new package.

2.40. RHEA-2011:0575 — new package: slapi-nis

A new slapi-nis package is now available for Red Hat Enterprise Linux 6.

The slapi-nis package provides two plug-ins for the 389 Directory Server and Red Hat Directory Server: The NIS Server plug-in allows a directory server to serve its data to clients using the NIS protocol. The Schema Compatibility plug-in allows a directory server to provide a modified view of a set of entries in a designated section of the directory.

This enhancement update adds the slapi-nis package to Red Hat Enterprise Linux 6. (BZ#643558)

All users who require slapi-nis should install this new package.

2.41. RHEA-2011:0585 — new package: spice-protocol

A new spice-protocol package is now available for Red Hat Enterprise Linux 6.

The spice-protocol package contains header files that describe the SPICE protocol and the QXL para-virtualized graphics card. Spice-protocol is needed to build newer versions of the spice-client and spice-server packages.

This enhancement update adds the spice-protocol package to Red Hat Enterprise Linux 6. (BZ#662992)

Users who wish to build SPICE from source are advised to install this new package.

2.42. RHEA-2011:0576 — new package: spice-vdagent

A new spice-vdagent package is now available for Red Hat Enterprise Linux 6.

The new spice-vdagent package provides a SPICE agent for Linux guests.

Bug Fixes

BZ#658464

The new spice-vdagent package allows for client window mode, automatic X session resolution adjustment to the client resolution, and copy and paste support for text and images between a guest's active X session and the SPICE client operating system.

BZ#680227

guest resolutions were not automatically aligned when multiple monitors were used. This update corrects the monitor settings. Now, the vdagent automatically aligns the guest resolution for one and more monitors.

All SPICE virtual machines users should install this new package, which adds these features. Note: guests must be rebooted after installing this package for the changes to take effect.

2.43. RHEA-2011:0611 — new package: subscription-manager

New subscription-manager packages that provide GUI and command line tools for the new Subscription Manager system are now available for Red Hat Enterprise Linux 6.

The new Subscription Management tooling will allow users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

This enhancement update adds new subscription-manager packages to Red Hat Enterprise Linux 6. (BZ#567635)

All users should install these newly-released packages, which add this enhancement.

2.44. RHEA-2011:0532 — new package: svrcore

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

The svrcore package contains an API library which provides various methods of handling and managing secure Personal Identification Number (PIN) storage. The svrcore library uses the Mozilla NSS cryptographic library. An example of an application which would use svrcore is one that must be restarted without user intervention, but which requires a PIN to unlock a private key and other cryptographic objects.

This enhancement update adds a new svrcore package to Red Hat Enterprise Linux 6. (BZ#643539)

All users requiring svrcore should install this newly-released package.

2.45. RHEA-2011:0727 — new package: system-switch-java

A new system-switch-java package is now available for Red Hat Enterprise Linux 6.

The system-switch-java package provides a tool that allows you to select the Java environment you want to use from the list of the installed Java alternatives. The tool supports a graphical user interface (GUI) and text user interface (TUI) mode.

This enhancement update adds the system-switch-java package to Red Hat Enterprise Linux 6. (BZ#663322)

All users who require system-switch-java should install this new package.

2.46. RHEA-2011:1442 — 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.

This enhancement update adds the tdb-tools packages to Red Hat Enterprise Linux 6. (BZ#717690)

All tdb users who wish to backup and manage tdb files are advised to install these new packages.

2.47. RHEA-2011:0657 — new package: tomcatjss

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

The tomcatjss package provides a Java Secure Socket Extension (JSSE) implementation using Java Security Services (JSS) for Tomcat 6.

This enhancement update provides the Java Native Interface (JNI) extension for JSS based on Network Security Services (NSS). (BZ#643544)

All tomcat users who wish to use NSS for servlet connectors are advised to install this new package.

2.48. RHEA-2011:0604 — new package: virt-what

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

The virt-what tool is used to detect whether the operating system is running inside a virtual machine.

This enhancement update adds a new virt-what package to Red Hat Enterprise Linux 6. The virt-what utility enables programs to detect if they are running in a virtual machine, as well as details about the type of hypervisor. (BZ#627886)

All users requiring virt-what should install this newly-released package, which adds this enhancement.

3. TECHNOLOGY PREVIEWS

Open Multicast Ping (Omping)

Open Multicast Ping (Omping) is a tool to test the IP multicast functionality primarily in the local network. This utility allows users to test multicast and assists in the diagnosing if an issues is in the

network configuration or elsewhere (i.e. a bug). In Red Hat Enterprise Linux 6 omping is provided as a Technology Preview.

Matahari

Matahari provides a set of Application Programming Interfaces (APIs) for operating systems management for remote access over QMF/QPID. In Red Hat Enterprise Linux 6.1, Matahari is considered a Technology Preview feature.

System Information Gatherer and Reporter (SIGAR)

The System Information Gatherer and Reporter (SIGAR) is a library and command-line tool for accessing operating system and hardware level information across multiple platforms and programming languages. In Red Hat Enterprise Linux 6.1, SIGAR is considered a Technology Preview package.

fsfreeze

Red Hat Enterprise Linux 6 includes **fsfreeze** as a Technology Preview. **fsfreeze** is a new command that halts access to a 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.

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

LVM Application Programming Interface (API)

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

FS-Cache

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

eCryptfs File System

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

IPv6 support in IPVS

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

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.

XFS in the Red Hat Enterprise Linux 6 High Availability Add On

XFS filesystem failover in the Red Hat Enterprise Linux 6 High Availability Add-On is considered a Technology Preview. Note: XFS and the Scalable File System Add-On are fully-supported in Red Hat Enterprise Linux 6.

upd-unicast support

Cluster membership can now be initiated using udp-unicast (UDPU). The older protocol (multicast) is often restricted by corporate IT policy, making it difficult to deploy clusters. Introducing UDPU support alliviates that limitation. This feature is considered a Technology Preview in Red Hat Enterprise Linux 6.1.

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.

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.

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.

Kernel Media support (Tech Preview)

- Very current upstream video4linux
- Digital video broadcasting
- Primarily infrared remote control device support
- Many webcam support fixes and improvements

Remote Audit Logging

The audit package contains the user space utilities for storing and searching the audit records generated by the audit subsystem in the Linux 2.6 kernel. Within the audispd-plugins subpackage is a utility that allows for the transmission of audit events to a remote aggregating machine. This remote audit logging application, audisp-remote, is considered a Technology Preview in Red Hat Enterprise Linux 6.

Linux (NameSpace) Container [LXC]

Linux (NameSpace) Containers [LXC] is a Technology Preview feature in Red Hat Enterprise Linux 6 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.

Diagnostic pulse for the fence_ipmilan agent

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

4. KNOWN ISSUES

4.1. Installer

- 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.
- 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.

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

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

- 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.

4.2. Deployment

- In Red Hat Enterprise Linux 6.1, multilib Python packages and packages dependent on them have been removed. This was because installing Python packages for multiple architectures on one system can cause various problems. For more information, refer to https://access.redhat.com/site/solutions/68140.

- 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".

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

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

- Parted 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.

4.3. Virtualization

- 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.

- 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.

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

- 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.

- 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.

- 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.

- 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.

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

4.4. Storage and Filesystems

- 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.

- 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.

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

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

Mirror logs can be handled in a similar fashion:

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

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

4.5. Networking

- 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`**.

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

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

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

4.6. Clustering

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

4.7. Authentication

- SSSD currently does not support eDirectory account lockout policies.
- when installing a replica (using the ipa-replica-install command), GSSAPI errors similar to the following might be returned:

```
[07/Apr/2011:10:46:23 -0400] slapi_ldap_bind - Error: could not
perform interactive bind for id [] mech [GSSAPI]: error -2 (Local
error)
[07/Apr/2011:10:46:23 -0400] NSMMReplicationPlugin -
agmt="cn=meToipaqa64vmb.testrelm" (ipaqa64vmb:389): Replication bind
with GSSAPI auth failed: LDAP error -2 (Local error) (SASL(-1):
generic failure: GSSAPI Error: Unspecified GSS failure.  Minor code
may provide more information (Credentials cache file
'/tmp/krb5cc_496' not found))
```

  These messages can be safely ignored.

4.8. Devices

- The Emulex lpfc driver should not be unloaded. If the driver is unloaded, a system crash might occur.
- 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.
- 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.

4.9. Kernel

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

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

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

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

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

- Loading the megaraid_sas driver on the kdump kernel will result in the insmod command being blocked, returning messages similar to:

  ```
  INFO: task insmod:201 blocked for more than 120 seconds.
  ```

  Refer to BZ#682110 for more information.

- In Red Hat Enterprise Linux 6.1, the nmi_watchdog registers with the perf subsystem. Consequently, during boot, the perf subsystem grabs control of the performance counter registers, blocking oprofile from working. To resolve this, either boot with the **nmi_watchdog=0** kernel parameter set, or run **echo 0 > /proc/sys/kernel/nmi_watchdog** to disable at run time. To re-enable the watchdog, use the command **echo 1 > /proc/sys/kernel/nmi_watchdog**.

- 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
  ```

- 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.

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

- On IBM PowerPC systems, the exec-shield value in sysctl or /proc/sys/kernel/exec-shield parameter is not enforced.

4.10. Desktop

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

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

- Evolution'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.

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

- 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.

- 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"
```

A. REVISION HISTORY

Revision 1-4 **Wed Feb 25 2015** **Laura Bailey**

Rebuild for sort order.

Revision 1-3.7 **Wed Jan 22 2014** **Eliška Slobodová**

Added the missing eCryptfs Technology Preview.

Revision 1-3.5 **Mon Jun 17 2013** **Eliška Slobodová**

Fixed broken links and links pointing to the old Product Documentation site.

Revision 1-3.3 **Thu Dec 13 2012** **Martin Prpič**

Added a note about removal of multilib Python packages.

Revision 1-3.1 **Wed May 20 2012** **Martin Prpič**

Republished Technical Notes to update list of included advisories. For more information, refer to the Important note in the *Package Updates* chapter of this book.

Revision 1-2 **Mon May 23 2011** **Ryan Lerch**

Updated Technology Previews section, Removed references to 'Beta' and Updated the XFS on High Availability Technology Preview note.

Revision 1-1 **Thu May 19 2011** **Ryan Lerch**

Initial Release of the Red Hat Enterprise Linux 6.1 Technical Notes