Red Hat Enterprise Linux 5
5.4 Technical Notes

Every Change to Every Package
Edition 4

Red Hat Inc.

Red Hat Enterprise Linux 5 5.4 Technical Notes

Every Change to Every Package
Edition 4

Legal Notice

Abstract

The Red Hat Enterprise Linux 5.4 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 5.3 and minor release Red Hat Enterprise Linux 5.4.

Table of Contents

Preface

The Red Hat Enterprise Linux 5.4 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 5.3 and minor release Red Hat Enterprise Linux 5.4.

For system administrators and others planning Red Hat Enterprise Linux 5.4 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 5.4 Technical Notes provide a single, organized source for change tracking and compliance testing.

For every user, the Red Hat Enterprise Linux 5.4 Technical Notes provide details of what has changed in this new release.

The Technical Notes also include, as an Appendix, the Red Hat Enterprise Linux Package Manifest: a listing of every changed package in this release.

Chapter 1. Package Updates

1.1. NetworkManager

1.1.1. RHSA-2009:0361: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0361

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

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

NetworkManager is a network link manager that attempts to keep a wired or wireless network connection active at all times.

An information disclosure flaw was found in NetworkManager's D-Bus interface. A local attacker could leverage this flaw to discover sensitive information, such as network connection passwords and pre-shared keys. (CVE-2009-0365)

A potential denial of service flaw was found in NetworkManager's D-Bus interface. A local user could leverage this flaw to modify local connection settings, preventing the system's network connection from functioning properly. (CVE-2009-0578)

Red Hat would like to thank Ludwig Nussel for reporting these flaws responsibly.

Users of NetworkManager should upgrade to these updated packages which contain backported patches to correct these issues.

1.1.2. RHBA-2009:1389: bug fix update

Updated NetworkManager packages that fix several bugs are now available.

NetworkManager is a network link manager that attempts to keep a wired or wireless network connection active at all times.

These updated NetworkManager packages provide the following fixes:

- NetworkManager allowed users to create completely insecure ad-hoc wireless networks and indeed, the default security setting for wifi sharing was "none". Because of this default setting and because NetworkManager did not warn users of the potential security risks, users could unwittingly compromise the security of their computers. Now, NetworkManager uses "WEP Passphrase" as the default security option for creating a new wifi network, and allows administrators to disable users' ability to share wifi connections without security in place, or their ability to share wifi connections at all. These measures make it less likely that a user could inadvertently compromise a sensitive system. (BZ#496247)
- accessing the context (right-click) menu of the NetworkManager GNOME applet could trigger the GNOME Keyring Unlock dialog to appear, after which no X11 applications could receive keyboard or mouse events. Now, NetworkManager closes the context menu before requesting keyring items, and therefore avoids this situation. (BZ#476020)

- NetworkManager did not export VPN configurations. When a user selected this function, NetworkManager would present an error message: "VPN setting invalid", even for a connection with valid settings. Network manager now exports VPN connections correctly. (BZ#485345)
- due to faulty logic in the code, nm-applet would choose the lowest signal strength of all APs of the same SSID in the area and display this strength in the menu to represent the signal strength for that SSID. NetworkManager now correctly calculates wireless signal strength when multiple access points with the same SSID are present. (BZ#485477)
- when NetworkManager fails to connect to a wifi network, it re-prompts the user for the passphrase for that network. Previously, NetworkManager did not retain the original text of the passphrase entered by the user. Therefore, when users selected the "Show password" option so that they could see what they had typed after a failed connection attempt, NetworkManager displayed the passphrase in hexadecimal form. NetworkManager now retains the original text of the passphrase and displays the original passphrase instead of a hexadecimal string when the user selects the "Show password" option. (BZ#466509)
- NetworkManager has its own internal method of starting loopback devices, and does not use the configuration settings stored in /etc/sysconfig/network-scripts/ifcfg-lo. Previously, NetworkManager would produce an error, alerting users that the configuration settings were ignored. This error message could mislead users to think that a problem had occurred. Now, NetworkManager does not present this error message to the user, and avoids the potential confusion. (BZ#484060)
- the NetworkManager package requires wpa_supplicant, but previously omitted the Epoch term for the wpa_supplicant package. Consequently, installing NetworkManager did not ensure that a suitable version of wpa_supplicant was installed on the system. Now, the NetworkManager package specifies the epoch for the version of wpa_supplicant that it requires. (BZ#468688)
- NetworkManager displayed configuration options for VPN even when no VPN software was installed on the system. This could mislead users to think that they could make VPN connections in situations when it was not possible to make these connections. Now, the VPN submenu is hidden if no VPN services are installed on the system, avoiding the potential confusion. (BZ#464604)

Users are advised to upgrade to these updated NetworkManager packages, which provide these fixes.

1.2. OpenIPMI

1.2.1. RHEA-2009:1312: bug fix and enhancement update

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

OpenIPMI (Intelligent Platform Management Interface) provides graphical and command line tools and utilities to access platform information, thus facilitating system management and monitoring for system administrators.

These updated packages upgrade OpenIPMI to upstream version 2.0.16 and ipmitool to version 1.8.11. (BZ#475542)

These updated OpenIPMI packages provide fixes for the following bugs:

- some IPMI-enabled hardware makes use of UDP ports 623 (ASF Remote Management and Control Protocol) and 664 (ASF Secure Remote Management and Control Protocol), which corrupts other traffic on these ports, causing symptoms such as autofs mounts hanging. The OpenIPMI package provides a configuration file for xinetd that prevents other services from using these ports, so that they do not interfere with IPMI. On affected systems, the fix has to be enabled manually by setting "disabled = no" for the appropriate port(s) in /etc/xinetd.d/rmcp and (re)starting the xinetd service. (BZ#429329)

- on the S/390 architecture, running "ipmicmd" to access the internal hash table of open connections caused the utility to segmentation fault. With this update, "ipmicmd" correctly handles the hash table and thus no longer crashes. (BZ#437013)
- the "rmcp_ping" utility did not perform checks on the arguments provided to it on the command line, and would accept invalid port numbers and/or start tags. (BZ#437256)
- the ipmitool utility is shipped in the OpenIPMI-tools packages, and it was not possible to have other packages depend on "ipmitool" directly. These updated packages explicitly provide the "ipmitool" feature so that other packages are now able to reference it. (BZ#442784)
- several libraries in the OpenIPMI packages contained unnecessary RPATH values, which have not been compiled in to these updated packages. (BZ#466119)
- the OpenIPMI-devel packages contained manual pages which were already provided by the OpenIPMI packages and have therefore been removed from the OpenIPMI-devel packages. (BZ#466487)
- the ipmievd daemon listens for events sent by the BMC to the SEL and logs those events to syslog. Previously, the OpenIPMI-tools package did not contain the init script for the "ipmievd" service. This init script is included in these updated packages. (BZ#469979)
- previously, it was not possible to query "ipmitool" to determine whether SOL payloads were enabled or disabled for specific users. These updated packages introduce a new "ipmitool sol payload status" query that implements the "Gets User Payload Access Command" from the IPMI specification, thus allowing users' SOL payload access privileges to be queried. (BZ#470031)
- the "ipmitool sel list" command displayed event IDs as hexadecimal numbers. However, it was not possible to then provide these values as parameters to other "ipmitool sel" commands. These packages include an updated ipmitool whose various "ipmitool sel" commands accept both decimal and hexadecimal ID values as parameters. (BZ#470805)
- it was not possible to specify a Kg key with non-printable characters on the ipmitool command line. With this update, a Kg key can now be specified as a hexadecimal value using the '-y' command line option. (BZ#479252)
- the "sensor list" section of the ipmitool(1) man page now describes each columnar value of the command "ipmitool sensors list". (BZ#479702)

In addition, these updated packages provide the following enhancements:

- new in this OpenIPMI 2.0.16 release is the OpenIPMI-gui package, which contains a GUI that provides a tree-structured view of the IPMI domains it is connected to. (BZ#504783)
- the "ipmitool sol set" command now checks the values of arguments provided on the command line. (BZ#311231)
- the ipmitool(1) man page has been updated to include descriptions for these commands: spd, picmg, hpm, firewall, fwum and kontronoem. (BZ#438539)

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

1.3. acpid

1.3.1. RHSA-2009:0474: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0474

An updated acpid package that fixes one security issue is now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

acpid is a daemon that dispatches ACPI (Advanced Configuration and Power Interface) events to user-space programs.

Anthony de Almeida Lopes of Outpost24 AB reported a denial of service flaw in the acpid daemon's error handling. If an attacker could exhaust the sockets open to acpid, the daemon would enter an infinite loop, consuming most CPU resources and preventing acpid from communicating with legitimate processes. (CVE-2009-0798)

Users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

1.3.2. RHBA-2009:1403: bug fix update

An updated acpid package that fixes a bug is now available.

acpid is a daemon that dispatches ACPI (Advanced Configuration and Power Interface) events to user-space programs.

In some pre-release versions of Red Hat Enterprise Linux 5.4, the Hardware Abstraction Layer (HAL) daemon was initialized before the ACPI daemon. Consequently, this resulted in the HAL daemon preventing the ACPI daemon from accessing /proc/acpi/event. With this update, the acpid package has been updated so the ACPI daemon now starts before the HAL daemon, which resolves this issue. (BZ#503177)

Users should upgrade to this updated package, which resolves these issues.

1.4. acroread

1.4.1. RHSA-2009:1109: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1109

Updated acroread packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3 Extras, Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

Multiple security flaws were discovered in Adobe Reader. A specially crafted PDF file could cause Adobe Reader to crash or, potentially, execute arbitrary code as the user running Adobe Reader when opened.

(CVE-2009-0198, CVE-2009-0509, CVE-2009-0510, CVE-2009-0511, CVE-2009-0512, CVE-2009-0888, CVE-2009-0889, CVE-2009-1855, CVE-2009-1856, CVE-2009-1857, CVE-2009-1858, CVE-2009-1859, CVE-2009-1861, CVE-2009-2028)

All Adobe Reader users should install these updated packages. They contain Adobe Reader version 8.1.6, which is not vulnerable to these issues. All running instances of Adobe Reader must be restarted for the update to take effect.

1.4.2. RHSA-2009:0478: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0478

Updated acroread packages that fix two security issues are now available for Red Hat Enterprise Linux 3 Extras, Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

Two flaws were discovered in Adobe Reader's JavaScript API. A PDF file containing malicious JavaScript instructions could cause Adobe Reader to crash or, potentially, execute arbitrary code as the user running Adobe Reader. (CVE-2009-1492, CVE-2009-1493)

All Adobe Reader users should install these updated packages. They contain Adobe Reader version 8.1.5, which is not vulnerable to these issues. All running instances of Adobe Reader must be restarted for the update to take effect.

1.4.3. RHSA-2009:0376: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0376

Updated acroread packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3 Extras, Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

Multiple input validation flaws were discovered in the JBIG2 compressed images decoder used by Adobe Reader. A malicious PDF file could cause Adobe Reader to crash or, potentially, execute arbitrary code as the user running Adobe Reader. (CVE-2009-0193, CVE-2009-0658, CVE-2009-0928, CVE-2009-1061, CVE-2009-1062)

All Adobe Reader users should install these updated packages. They contain Adobe Reader version 8.1.4, which is not vulnerable to these issues. All running instances of Adobe Reader must be restarted for the update to take effect.

1.5. aide

1.5.1. RHEA-2009:1073: enhancement update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHEA-2009:1073

An enhanced aide package that contains minor adjustments to the aide.conf configuration file to offer improved initial behavior is now available.

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

This updated aide package adds the following enhancement:

- the /var/run/utmp configuration file is now correctly treated as a log file, and the hidden files (also known as "dot files") located in the root user's home directory are now checked for permission integrity only. These enhancements to AIDE should cause systems to produce fewer false alarms concerning files which have changed. (BZ#476542)

Users of aide are advised to upgrade to this updated package, which adds this enhancement.

1.6. amanda

1.6.1. RHBA-2009:1300: bug fix update

Updated amanda packages that fix two bugs are now available.

Amanda is a network-capable tape backup solution.

These updated amanda packages resolve the following issues:

- the "amtapetype" command had a bug in memory management: an invalid pointer was passed to the free() function. In some circumstances this caused amrecover to fail with a "Extractor child exited with status 2" error. The invalid pointer is no longer passed to free() and amrecover extracts files from a tape backup as expected. (BZ#476971)

- previously, amanda sub-packages (including amanda-devel, amanda-server and amanda-client) were only required to be the same version as amanda: they did not check that their release was in sync with the base amanda package. This could cause the packages to go out-of-sync and malfunction if an attempt was made to update either the base amanda package or any of amanda's sub-packages. With this update, both the version and release are checked, ensuring all dependent packages remain in sync if either the base package or any sub-packages are updated. (BZ#497111)

Users of amanda should upgrade to these updated packages, which resolves these issues.

1.7. anaconda

1.7.1. RHBA-2009:1306: bug fix and enhancement update

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

Anaconda is the system installer.

These updated anaconda packages provide fixes for the following bugs:

Anaconda is the system installer.

These updated anaconda packages provide fixes for the following bugs:

- a write-protected SD card could cause an installation failure even when the mount point was de-selected in the Disk Druid. (BZ#471883)
- Anaconda occasionally attempted to delete nonexistent snapshots, which caused installation to fail. (BZ#433824)
- if a boot file was retrieved via DHCP, Anaconda now saves it so that it can later be used to construct the default Kickstart file if the user boots with "ks" as a boot parameter. (BZ#448006)
- driver disk locations can now be specified using the "dd=[URL]" option, where [URL] is an FTP, HTTP or NFS location. (BZ#454478)
- the bootloader can now be located in the MBR on a software RAID1 boot partition. (BZ#475973)
- Anaconda now installs multipath packages so that multipath devices work as expected following first reboot. (BZ#466614)
- Anaconda prompted for the time zone even when the time zone was correctly specified in the Kickstart file. (BZ#481617)
- on Itanium systems, the time stamps of installed files and directories were in the future. (BZ#485200)
- the iSCSI Boot Firmware Table (iBFT) now works with Challenge-Handshake Authentication Protocol (CHAP) and reverse-CHAP setups. (BZ#497438)
- Anaconda now correctly sets the umask on device nodes. (BZ#383531)
- following a manual installation during which IPv6 was configured, the /etc/sysconfig/network-scripts/ifcfg-[interface] file (such as ifcfg-eth0) did not contain those IPv6 network details. (BZ#445394)
- Anaconda now correctly handles LAN channel station (LCS) devices. (BZ#471101)
- when using autostep mode with a Kickstart configuration file, Anaconda incorrectly prompted for a root password even when the root password was designated as encrypted. (BZ#471122)
- empty repositories caused installation to fail. (BZ#476182)
- large numbers of tape drives in the Kickstart file are now handled correctly. (BZ#476186)
- hyphenated MAC address formats in the Kickstart file (e.g. "ksdevice=00-11-22-33-44-55") are now allowed. (BZ#480309)
- an unexpected exception during Logical Unit Number (LUN) selection caused installation to fail. (BZ#475271)
- when installing on a low-memory system or virtual machine over HTTP or FTP, a non-present "lspci" binary caused installation to fail. (BZ#476476)
- Anaconda now correctly adds the user to the default group, and groups specified by "--groups", when performing a Kickstart installation. (BZ#454418)

- the "cmdline" option, which specifies a non-Ncurses installation, is now honored in the Kickstart file. (BZ#456325)
- Kickstart file download from an anonymous FTP site is now possible. (BZ#477536)

In addition, these updated packages provide the following enhancements:

- default configuration values are now suggested during System z installation. (BZ#475350)
- hardware device descriptions have been enhanced to reflect expanded hardware support. (BZ#498511)
- the Mellanox ConnectX mt26448 10Gb/E driver is now supported. (BZ#514971)
- the mpt2sas driver is now supported. (BZ#475671)
- the Emulex Tiger Shark converged network adatper is now supported. (BZ#496875)
- the Marvell RAID bus controller MV64460/64461/64462 and Emulex OneConnect 10GbE NIC devices are now supported. (BZ#493179)
- the IGB Virtual Function driver is now supported. (BZ#502875)
- installation on RAID10 devices is now supported. (BZ#467996)
- non-fatal errors and conditions are now ignored when installing from a Kickstart file. (BZ#455465)
- stale LVM metadata can now be removed with the "--clearpart" option. (BZ#462615)
- to aid in identifying the network card, an option to blink its LED for 5 minutes is now present. (BZ#473747)
- IPv6 address validation on S/390 installations has been improved. (BZ#460579)

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

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

1.8. apr

1.8.1. RHSA-2009:1204: Moderate and apr-util security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1204

Updated apr and apr-util packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. It aims to provide a free library of C data structures and routines. apr-util is a utility library used with APR. This library provides additional utility interfaces for APR; including support for XML parsing, LDAP, database interfaces, URI parsing, and more.

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the way the Apache Portable Runtime (APR) manages memory pool and relocatable memory allocations. An attacker could use these flaws to issue a specially-crafted request for memory allocation, which would lead to a denial of service (application crash) or, potentially, execute arbitrary code with the privileges of an application using the APR libraries. (CVE-2009-2412)

All apr and apr-util users should upgrade to these updated packages, which contain backported patches to correct these issues. Applications using the APR libraries, such as httpd, must be restarted for this update to take effect.

1.9. apr-util

1.9.1. RHSA-2009:1107: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1107

Updated apr-util packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

apr-util is a utility library used with the Apache Portable Runtime (APR). It aims to provide a free library of C data structures and routines. This library contains additional utility interfaces for APR; including support for XML, LDAP, database interfaces, URI parsing, and more.

An off-by-one overflow flaw was found in the way apr-util processed a variable list of arguments. An attacker could provide a specially-crafted string as input for the formatted output conversion routine, which could, on big-endian platforms, potentially lead to the disclosure of sensitive information or a denial of service (application crash). (CVE-2009-1956)

Note: The CVE-2009-1956 flaw only affects big-endian platforms, such as the IBM S/390 and PowerPC. It does not affect users using the apr-util package on little-endian platforms, due to their different organization of byte ordering used to represent particular data.

A denial of service flaw was found in the apr-util Extensible Markup Language (XML) parser. A remote attacker could create a specially-crafted XML document that would cause excessive memory consumption when processed by the XML decoding engine. (CVE-2009-1955)

A heap-based underwrite flaw was found in the way apr-util created compiled forms of particular search patterns. An attacker could formulate a specially-crafted search keyword, that would overwrite arbitrary heap memory locations when processed by the pattern preparation engine. (CVE-2009-0023)

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

1.10. aspell

1.10.1. RHBA-2009:1070: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1070

An updated aspell-nl package that fixes a bug is now available.

Aspel-nl provides the word list/dictionaries for Dutch language.

This updated aspell-nl package fixes the following bug:

- the previous aspell-nl update provided also an empty aspell-nl-debuginfo package. The dictionary packages for Aspell do not require debuginfo packages; this update therefore removes the extraneous aspell-nl-debuginfo package. (BZ#500540)

All Dutch language Aspell users are advised to upgrade to this updated package, which resolves this issue.

1.11. audit

1.11.1. RHBA-2009:0475: bug fix and enhancement update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0475

Updated audit packages that fix a bug and add an enhancement are now available.

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

These updated audit packages fix the following bug:

- ausearch was unable to interpret tty audit records. tty records are specially-encoded, and the ausearch program could not decode them, which resulted in their being displayed in encoded form. These updated packages enable ausearch to interpret (i.e. decode correctly) TTY records, thus resolving the issue. (BZ#497518)

In addition, these updated audit packages provide the following enhancement:

- The aureport program was enhanced to add a '--tty' report option. This is a new report that was recently added to audit in order to aid in the review of TTY audit events. (BZ#497518)

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

1.11.2. RHBA-2009:0443: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0443

Updated audit packages that resolve several issues are now available.

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

These updated packages fix the following bugs in the auditd daemon and one of its utilities:

- when the log_format parameter was set to "NOLOG" in the auditd.conf configuration file, audit events which were queued in the internal message queue were not cleared after being written to dispatchers. This caused the internal message queue to grow over time, causing an auditd memory leak. With these updated packages the audit events in the internal message queue are properly cleared after being written, thus plugging the memory leak.

- certain audit rules failed parser checks even though they were specified correctly, which prevented those rules from being loaded into the kernel. With this update, all correctly-specified audit rules pass parser checks and can be loaded into the kernel, thus resolving the problem.

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

1.11.3. RHEA-2009:1303: enhancement

Updated audit packages, which includes TTY audit and remote log aggregation updates among other enhancements, are now available.

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

These updated packages upgrade the auditd daemon and its utilities to the newer upstream version 1.7.13 (BZ#483608), which provides the following enhancements and bug fixes over the previous version:

- the user-space audit tools use ausearch to search audit records. Ausearch does not contain logic to handle event-linked lists and previously, could not find records if they were out of chronological order. The logic to link these lists together and evaluate whether the list is complete is now available in the auparse library. Ausearch now uses auparse to handle these lists so that it can find records even when they are out of order. (BZ#235898)

- the manual page for ausyscall did not document use of the "--exact" option. A description of "--exact" is now included. (BZ#471383)

- due to a logic error, the "local_port = any" option for the audisp-remote plugin did not work as described in the manual page. When executed with this option, the plugin would display the error "Value any should only be numbers" and terminate. With the error corrected, the plugin works as documented. (BZ#474466)

- previously, audisp would read not only its configuration file (in /etc/audisp/plugins.d/) but any files with names simlar to its configuration file found in the same directory, for example, backups of the configuration file. As a result, if a plugin were listed in more than one configuration file, it would be activated multiple times. audisp now reads only its configuration file and therefore avoids activating multiple copies of plugins. (BZ#476189)

- previously, TTY audit results were reported in ausearch in their raw hexadecimal form. This format was not easily readable by humans, so ausearch now converts the hexadecimal strings and presents them as their corresponding keystrokes. Note that the "--tty" option has now been added to aureport to provide a convenient way of accessing the TTY audit report. (BZ#483086)

- previously, when setting the output log format to "NOLOG", audit events would be added to the internal message queue but not removed from the queue when written to the dispatchers. The queue would therefore grow to consume available memory. Audit events are now removed from the internal queue to avoid this memory leak. (BZ#487237)

- due to a logic error, auditctl was not correctly parsing options that included non-numeric characters. For example, the "-F a0!=-1" option would result in an error saying "-F value should be number for a0!=-1". With the error corrected, auditctl parses this rule correctly. (BZ#497542)

Other issues corrected in the rebase include:

- remote logging is a technology preview item and as such had some bugs. Robustness of this facility was improved.
- on busy systems, pam had problems communicating with the audit system, which resulted in a timeout and being denied access to the system. We now loop a few times when checking for the event ACK.
- On biarch system, a warning is emitted if audit rules don't cover both 64 & 32 bit syscalls of the same name.
- Fix regression where msgtype couldn't be used for a range of types.
- New aulast program helps analyse login session information.
- If log rotation fails, auditd now leaves the old log writable.
- A tcp_wrappers config option was added to auditd for remote logging.
- Fix problem where negative uids in audit rules on 32 bit systems resulted in the wrong uid and therefore incorrect event logging.

Users of audit are advised to upgrade to these updated packages, which add these enhancements and bug fixes.

1.12. authconfig

1.12.1. RHBA-2009:0482: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0482

Updated authconfig packages that fix a bug are now available.

The authconfig packages contain a program with both a command line and a GUI interface for configuring a system to use shadow passwords, or to function as a client for certain network user-information and authentication schemes.

- when disabling caching using the system-config-authentication graphical interface or with the "authconfig --update --disablecache" command, authconfig did not properly stop ncsd, the name service cache daemon, which could have caused timeouts and delays during authentication or when user information was requested by applications. (BZ#471642)

Users are advised to upgrade to these updated authconfig packages, which resolve this issue.

1.13. authd

1.13.1. RHBA-2009:0442: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0442

An updated authd package that fixes various bugs is now available.

The authd package contains a small and fast RFC 1413 ident protocol daemon with both xinetd server and interactive modes that supports IPv6 and IPv4 as well as the more popular features of pidentd.

This updated authd package includes fixes for the following bugs:

- on 64-bit architectures, a size mismatch between data structures led to an endlessly repeating pattern of output, though no error. This size mismatch has been fixed in this updated package so that authd works as expected.
- attempting to connect to a Postgresql database using identd authentication resulted in error messages similar to the following in Postgresql's pg_log, where [user] is the username of the user attempting to connect:

  ```
  CESTLOG:  invalidly formatted response from Ident server: "49795 ,
  5432 : ERROR :[user]
  ```

  This authd error has been corrected so that users are now able to log in successfully, thus resolving the issue.
- previously, installing the authd package resulted in the creation of a user named "ident" with a home directory of /home/ident. With this updated package, the "ident" user is still created, but, by convention, ident's home directory is the root ("/") directory.

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

1.14. autofs

1.14.1. RHBA-2009:1131: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1131

An updated autofs package that fixes a bug which caused autofs to fail occasionally when accessing an LDAP server while using SASL authentication is now available.

The autofs utility controls the operation of the automount daemon, which automatically mounts, and then unmounts file systems after a period of inactivity. File systems can include network file systems, CD-ROMs, diskettes, and other media.

This updated autofs package fixes the following bug:

- when connecting to an LDAP server while using SASL authentication, autofs occasionally failed with a segmentation fault, forcing users to restart the autofs service. This failure was caused by a double-free error in the cyrus-sasl module, which has been fixed in this updated package. Connecting to an LDAP server while using SASL authentication now works as expected. (BZ#504566)

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

1.14.2. RHBA-2009:1397: bug fix update

An updated autofs package that fixes various bugs and adds an enhancement is now available.

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.

- Previously, automount did not return its status to its parent while it waited for the autofs daemon to complete its startup. As a result, the init script did not always report success when the service started sucessfully. Automount now returns its status and accurately reports when the service has started. (BZ#244177)

- Autofs uses "umount -l" to clear active mounts at restart. This method results in getcwd() failing because the point from which the path is constructed has been detached from the mount tree. To resolve this a miscellaneous device node for routing ioctl commands to these mount points has been implemented in the autofs4 kernel module and a library added to autofs. This provides the ability to re-construct a mount tree from existing mounts and then re-connect them. (BZ#452122)

- Previously, the version of autofs shipped with Red Hat Enterprise Linux 5 used the "-hosts" method as its default way to handle /net mounts. Using this method, it was necessary to reboot the client to release processes if if the connection to the server was lost. Now, autofs uses the "intr" option as its default, which allows the mount to be unmounted forcibly if necessary. (BZ#466673)

- By default, autofs waits 60 seconds for a server to respond while performing a YP lookup. Previously, repeated attempts to perform lookups for non-existent directories could result in all available ports becoming congested. Autofs now maintains a cache of failed lookups and avoids repeated failures occupying the available ports. (BZ#469387)

- The %{dist?} tag that is used by rpm spec files is defined in ~/.rpmmacros for the user building the package. However, this is not a reliable method of providing the "Release:" tag in a package, because the {%dist?} tag might not be defined for the user building the package. Previously, autofs relied on the {%dist?} tag to define "Release:" in its spec file, which meant that building it correctly depended on the user's ~/.rpmmacros file being set up appropriately. "Release:" is now defined directly in the autofs file system, which makes it more likely to build correctly on a greater number of systems. (BZ#471385)

- Previously, the LDAP module lacked the ability to lock the server list. When used in SASL authenticated environments, this could cause autofs to fail if the credential for the connection became stale. The LDAP module can now lock a server list, and autofs refreshes and retries failed SASL connections. Autofs therefore performs more reliably when used in authenticated environments. (BZ#481139)

- Submounts are detached threads that do not belong to the master map entry list. Previously, autofs did not release mount resources when a mount thread for a submount was terminated. With these resources not released, a segmentation fault during a shutdown or reboot of the system could result. Resources allocated to submounts are now explictly released in the code and the segmentation fault is therefore avoided. (BZ#482988)

- Previously, autofs contained an an incorrect %token declaration in the master map parser. In some rare cases this could cause the timeout sent from the tokenizer to the parser to always be zero, which is interpreted as "never". As a result, indirect mounts would never expire, no matter how long they had been inactive. The %token declaration is now corrected, meaning that mounts expire as they should. (BZ#487151)

- Previously, autofs used the select() function to process direct-mount maps and was therefore limited by the file descriptor limit (by default, 1024). As a consequence, autofs was not able to use direct-mount maps with numbers of entries larger than the limit, and would stop responding when it used up all available file descriptors. Now, autofs uses poll() instead of select() and is therefore no longer limited by the available file descriptors. Freed of this limitation, autofs can use large direct-mount maps. (BZ#487653)

- Previously, autofs reported an incorrect buffer size internally when passing the startup status from the autofs daemon to the parent process. Although no specific consequences of this inaccuracy are known, the buffer size is now reported correctly to avoid any consequences arising in the future. (BZ#487656)

- Previously, the additive hashing algorithm used by autofs to generate hash values would result in a clustering of values that favoured a small range of hash indexes and led to reduced performance in large maps. Autofs now uses a "one-at-a-time" hash function which gives a better distribution of hash values in large hash tables. Use of the "one-at-a-time" hash function safeguards lookup performance as maps increase to 8,000 entries and beyond. (BZ#487985)

- Previously, autofs would not always read file maps. If a map had been loaded into cache, autofs would rely on checks to determine whether the map was up to date before reading the map. Because file maps require a linear search through the file, large maps consume significant resources to process. Now, autofs automatically loads file-based maps when it starts, and uses the map file mtime parameter to detemine whether the cache needs to be refresed. This avoids the processing overhead of checking a map before deciding whether to load it. (BZ#487986)

- Previously, the autofs code contained a logic error that resulted in a crash under conditions of heavy load. When autofs was not able to create a new pthread, it would double free a value. Now, with the error corrected, when heavily loaded, autofs will fail to create a new pthread safely. It reports the failure, but does not crash. (BZ#489658)

- Previously, autofs could use the LDAP server on a network only if the location of the LDAP server were specified manually. Now, if no LDAP server is specified, autofs can look up domain SRV server records to make LDAP connections. This functionality simplifies the use of autofs on networks where an LDAP server is available. (BZ#490476)

- Previously, if a name lookup failed while creating a TCP or UDP client, automount would destroy the client, but would not set the rpc client to NULL. Therefore, subsequent lookup attempts would attempt to use the invalid rpc client, which would lead to a segmentation fault. Now, when a name lookup fails, autofs sets the rpc client to NULL, and therefore avoids the segmentation fault on subsequent lookup attempts. (BZ#491351)

- Previously, in LDAP environments were both Red Hat Enterprise Linux and Solaris were in use, autofs would not correctly interpret master map keys added by Solaris. The auto_master file would therefore contain duplicate entries, where '%' symbols were interspersed between the characters of the map key names. Autofs now correctly parses the Solaris key names and does not create duplicate entries. (BZ#493074)

- Previously, a stack variable was not initialized on entry to the create_udp_client() or create_tcp_client() functions. During an error exit, the stack variable was checked, and the corresponding file descriptor was closed if the variable had a value other than -1. This could result in incorrectly closing a file descriptor still in use. The stack variable is now initialized and descriptors currently in use should not be closed. (BZ#493223)

- Due to a number of logic errors in the code, autofs could not remount a direct-mount NFS if the mount had expired following a map reload. The mount request would never complete, and "can't find map entry" would appear in the log. The logic errors are now fixed, and autofs can successfully remount an expired direct-mount NFS after a map reload. (BZ#493791)

- Previously, thread locking was missing from the st_remove_tasks() function, which meant in turn that its calling function could not get the locks that it required. This could result in a segmentation fault and a crash of autofs. Now, with the thread locking properly in place, the segmentation fault is avoided. (BZ#494319)
- Previously, when autofs looked up a host name where when one NFS server name was associated with multiple IP adresses, autofs would repeat the query many times. As a consequence of these multiple queries, the mount would take a long time. Now, redundant queries have been removed, so that autofs performs the mount more quickly. (BZ#495895)
- When connecting to an LDAP server while using SASL authentication, autofs occasionally failed with a segmentation fault, forcing users to restart the autofs service. This failure was caused by a double-free error in the cyrus-sasl module, which has been fixed in this updated package. Connecting to an LDAP server while using SASL authentication now works as expected. (BZ#501612)
- Previously, the method used by autofs to clean up pthreads was not reliable and could result in a memory leak. If the memory leak occurred, autofs would gradually consume all available memory and then crash. A small semantic change in the code prevents this memory leak from occurring now. (BZ#510530)

1.15. avahi

1.15.1. RHBA-2009:1119: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1119

Updated avahi packages that fix log output when invalid packets are received are now available.

Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zeroconf Networking. Avahi and Avahi-aware applications allow users to plug a computer into a network and automatically view other people to chat with, see printers to print to, and find shared files on other computers.

If Avahi receives an invalid mDNS packet, then it will write a message to syslog. The log message does not include the originating IP address of the packet, so it is not particularly useful to track down the source of the issue.

This update changes the log message to include the originating IP address of any invalid mDNS packets. This update also fixes some minor spelling errors in other log messages.

Users of avahi are advised to upgrade to these updated packages, which fix these issues.

1.16. bind

1.16.1. RHSA-2009:1179: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1179

Updated bind packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

[Updated 29th July 2009] The packages in this erratum have been updated to also correct this issue in the bind-sdb package.

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.

A flaw was found in the way BIND handles dynamic update message packets containing the "ANY" record type. A remote attacker could use this flaw to send a specially-crafted dynamic update packet that could cause named to exit with an assertion failure. (CVE-2009-0696)

Note: even if named is not configured for dynamic updates, receiving such a specially-crafted dynamic update packet could still cause named to exit unexpectedly.

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

1.16.2. RHBA-2009:1137: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1137

Updated bind packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

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.

These updated bind packages fix the following bug:

- DNSSEC, the Domain Name System Security Extensions, are a set of specifications used to secure information provided by the domain name system. One of the specifications, DNSSEC Lookaside Validation (DLV), failed to handle unknown algorithms, which caused the name resolution of "gov" and "org" top-level domains to fail. DLV in these updated packages is now able to handle unknown algorithms, and thus the validation and resolution of top-level domains (such as "org" and "gov") succeeds, thus resolving the issue. (BZ#504794)

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

1.16.3. RHBA-2009:1420: bug fix and enhancement update

Updated bind packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

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.

This update upgrades the bind packages to upstream version 9.3.6-P1, which contains bug fixes and enhancements over the previous version.

Notably, this updated BIND is able to handle a much larger number of requests simultaneously. (BZ#457036)

These updated bind packages provide fixes for the following bugs:

- named occasionally crashed due to an assertion failure, and logged this error message to the system log:

```
named[PID]: socket.c:1649: INSIST(!sock->pending_recv) failed
named[PID]: exiting
```

  This crash was caused by sockets being closed too early. With these updated packages, this assertion failure no longer occurs. (BZ#455802)

- when using the '-4' option with the "host" and "dig" utilities to force them to use an IPv4 transport, the order in which IPv4 and IPv6 nameservers were listed in the /etc/resolv.conf configuration file affected whether the command would fail or succeed. This has been fixed so that these utilities continue to look for an IPv4 address, even past listed IPv6 addresses, when the '-4' option is supplied. (BZ#469441)

- the "named-checkconf" utility ignored the "check-names" option in the /etc/named.conf configuration file, which caused the named daemon to fail to start, even if the configuration was valid. With these updated packages, "named-checkconf" no longer ignores the "check-names" option, and named starts up as expected. (BZ#491400)

- the named init script did not handle the named_write_master_zones SELinux boolean or the permissions on the /var/named/ directory as documented. (BZ#494370)

In addition, these updated packages provide the following enhancements:

- a new configuration directive which informs secondary servers not to send DNS notify messages, "notify master-only", is now supported. (BZ#477651)

- dynamic loading of database back-ends is now supported with these updated packages. (BZ#479273)

- the "allow-query-cache" option, which allows control over access to non-authoritative data (such as cached data and root hints), is now supported. (BZ#483708)

- the sample /etc/named.conf configuration file provided with these packages has been improved. (BZ#485393)

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

1.17. binutils

1.17.1. RHBA-2009:0465: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0465

Updated binutils packages that resolve several issues are now available.

binutils is a collection of utilities used for the creation of executable code.

These updated binutils packages provide fixes for the following bugs:

- the "objdump" and "size" utilities were not recognizing ELF64-i386 object files. Such files are not normally produced on 32-bit x86 architectures. However, the kdump utility does produce such files on Physical Address Extension (PAE)-enabled kernels. With these updated packages, it is now possible to use the objdump and size utilities on ELF64-i386 object files. (BZ#457189)
- due to a rare linking error, producing certain executables caused multi-megabyte zero-filled gaps in the executables. This did not affect the running of excutables affected by this bug. This linker error has been corrected in these updated packages so that executables do not contain spurious zero-filled gaps. (BZ#458301)
- the error message for the "strings -n [non-number]" command were less clear than in the previous package release, and therefore has been reverted and clarified. (BZ#480009)
- the c++filt(1) man page contained a typo when giving the syntax for the recognized '--strip-underscore' option. (BZ#485194)
- the c++filt(1) man page incorrectly mentioned the '-j' and '--java' options, which are not available when running c++filt. These mentionings have been removed from the man page. (BZ#495196)

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

1.18. busybox

1.18.1. RHBA-2009:1249: bug fix update

Updated busybox packages that resolve several issues are now available.

BusyBox combines tiny versions of many common UNIX utilities into a single small executable. It provides replacements for most of the utilities you usually find in GNU fileutils, shellutils, etc. BusyBox provides a fairly complete environment for any small or embedded system. This package can also be useful for recovering from certain types of system failures.

These updated busybox packages provide fixes for the following bugs:

- busybox provides a diff utility that is used extensively during installation. When this diff utility was called using the '-q' option, which reports only whether the files differ and not the details of how they differ, it always exited with an exit status of 0, indicating success. With this busybox update, the command "diff -q" correctly returns an exit status that corresponds to the same exit status returned when calling "diff" without the '-q' option, thus resolving the issue. (BZ#385661)
- invoking the "uname -p" command resulted in the processor type being listed as "unknown" when it should have been listed, for example, as "x86_64", or "i686". With these updated packages, "uname -p" either prints the processor type if known, or, if it is unknown, then the command is silent. This behavior now corresponds to the behavior of the uname command in coreutils. (BZ#480105)
- using BusyBox's rpm applet to install an rpm caused busybox to exit due to a segmentation fault caused by a memory corruption error. This has been fixed in these updated packages so that installing rpms using the "busybox rpm" command works as expected and does not fail with a segmentation fault. (BZ#466896)
- the busybox packages also contained empty debuginfo packages. These have been removed from this update. (BZ#500547)

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

1.19. cman

1.19.1. RHBA-2009:1192: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1192

Updated cman packages that fix various bugs are now available.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

This update applies the following bug fixes:

- Removing a node from the cluster using the 'cman_tool leave remove' command now properly reduces the expected_votes and quorum.
- Quickly starting and stopping the cman service no longer causes the cluster membership to become inconsistent across the cluster.

All cman users should upgrade to these updated packages, which resolve these issues.

1.19.2. RHBA-2009:1103: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1103

Updated cman packages that fix various bugs are now available.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

This update applies the following bug fixes:

- 'group_tool ls fence' no longer exits with return code '1' when the group exists but has an id of zero.
- Connections to openais are now allowed from an unprivileged CPG clients with the user 'ais' or an initial login group of 'ais'.

All cman users should upgrade to these updated packages, which resolve this issue.

1.19.3. RHBA-2009:0416: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0416

Updated cman packages that fix a bug are now available.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

This update applies the following bug fix:

- Nodes are no longer ejected from the cluster that were quorate on their own if they do not have a state.

All cman users should upgrade to these updated packages, which resolve this issue.

1.19.4. RHSA-2009:1341: Low security, bug fix, and enhancement update

Updated cman packages that fix several security issues, various bugs, and add enhancements are now available for Red Hat Enterprise Linux 5.

This update has been rated as having low security impact by the Red Hat Security Response Team.

The Cluster Manager (cman) utility provides services for managing a Linux cluster.

Multiple insecure temporary file use flaws were found in fence_apc_snmp and ccs_tool. A local attacker could use these flaws to overwrite an arbitrary file writable by a victim running those utilities (typically root) with the output of the utilities via a symbolic link attack. (CVE-2008-4579, CVE-2008-6552)

Bug fixes:

- a buffer could overflow if cluster.conf had more than 52 entries per block inside the <cman> block. The limit is now 1024.
- the output of the group_tool dump subcommands were NULL padded.
- using device="" instead of label="" no longer causes qdiskd to incorrectly exit.
- the IPMI fencing agent has been modified to time out after 10 seconds. It is also now possible to specify a different timeout value with the '-t' option.
- the IPMI fencing agent now allows punctuation in passwords.
- quickly starting and stopping the cman service no longer causes the cluster membership to become inconsistent across the cluster.
- an issue with lock syncing caused 'receive_own from' errors to be logged to '/var/log/messages'.
- an issue which caused gfs_controld to segfault when mounting hundreds of file systems has been fixed.
- the LPAR fencing agent now properly reports status when an LPAR is in Open Firmware mode.
- the LPAR fencing agent now works properly with systems using the Integrated Virtualization Manager (IVM).
- the APC SNMP fencing agent now properly recognizes outletStatusOn and outletStatusOff return codes from the SNMP agent.
- the WTI fencing agent can now connect to fencing devices with no password.
- the rps-10 fencing agent now properly performs a reboot when run with no options.
- the IPMI fencing agent now supports different cipher types with the '-C' option.
- qdisk now properly scans devices and partitions.
- cman now checks to see if a new node has state to prevent killing the first node during cluster setup.
- 'service qdiskd start' now works properly.
- the McData fence agent now works properly with the McData Sphereon 4500 Fabric Switch.
- the Egenera fence agent can now specify an SSH login name.
- the APC fence agent now works with non-admin accounts when using the 3.5.x firmware.

- fence_xvmd now tries two methods to reboot a virtual machine.
- connections to OpenAIS are now allowed from unprivileged CPG clients with the user and group of 'ais'.
- groupd no longer allows the default fence domain to be '0', which previously caused rgmanager to hang. Now, rgmanager no longer hangs.
- the RSA fence agent now supports SSH enabled RSA II devices.
- the DRAC fence agent now works with the Integrated Dell Remote Access Controller (iDRAC) on Dell PowerEdge M600 blade servers.
- fixed a memory leak in cman.
- qdisk now displays a warning if more than one label is found with the same name.
- the DRAC5 fencing agent now shows proper usage instructions for the '-D' option.
- cman no longer uses the wrong node name when getnameinfo() fails.
- the SCSI fence agent now verifies that sg_persist is installed.
- the DRAC5 fencing agent now properly handles modulename.
- QDisk now logs warning messages if it appears its I/O to shared storage is hung.
- fence_apc no longer fails with a pexpect exception.
- removing a node from the cluster using 'cman_tool leave remove' now properly reduces the expected_votes and quorum.
- a semaphore leak in cman has been fixed.
- 'cman_tool nodes -F name' no longer segfaults when a node is out of membership.

Enhancements:

- support for: ePowerSwitch 8+ and LPAR/HMC v3 devices, Cisco MDS 9124 and MDS 9134 SAN switches, the virsh fencing agent, and broadcast communication with cman.
- fence_scsi limitations added to fence_scsi man page.

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

1.20. cmirror

1.20.1. RHEA-2009:1340: bug-fix update

Updated cmirror packages that fix several bugs are now available.

The cmirror packages provide user-level utilities for managing cluster mirroring.

This update applies the following bug fixes:

- Copy percentage of corelog mirror no longer hangs due to stale checkpoint data.
- A segfault in clogd was fixed; the segfault was caused by mirrors being suspended too quickly after being started.

- The large number of dm-log-clustered timeouts generated by a pvmove no longer causes a cluster deadlock.
- Remnants of a moved device no longer remain in a volume group.
- Device-mapper userspace logs now have a local unique identifier to prevent issues when two logs have the same UUID.

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

1.21. cmirror-kmod

1.21.1. RHBA-2009:1367: bug fix update

Updated cmirror-kmod packages that fix a bug are now available.

The cmirror-kmod packages provide kernel-level interface for using cluster mirroring.

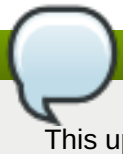
This update applies the following bug fix:

- kmod-cmirror packages now use symbols that are on the kernel ABI whitelist. (BZ#481689)

All users requiring cmirror-kmod should install these newly released packages, which resolve this issue.

1.22. conga

1.22.1. RHBA-2009:0381: bug fix update



Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0381

Updated conga packages that fix a bug are now available.

The conga packages contain a web-based administration tool for remote cluster and storage management.

These updated packages apply the following bug fix:

- A bug that prevented Microsoft Internet Explorer from working correctly with the Luci server has been fixed.

1.22.2. RHBA-2009:1381: bug-fix and enhancement update

Updated conga packages that fix several bugs and add enhancements are now available.

The conga packages contain a web-based administration tool for remote cluster and storage management.

This update applies the following bug fixes:

- A bug that caused some operations to fail when accessing Conga via Microsoft Internet Explorer was fixed.
- A bug that caused quorum disk heuristics to be lost after changing quorum disk main properties was fixed.

- A bug that made it impossible to set failover domains for virtual machine services was fixed.
- A bug that required that a fence device password be provided when a password script has been defined was fixed.
- A bug that caused the "run exclusive" cluster service attribute to always be shown as having been selected was fixed.
- A bug that caused adding existing Red Hat Enterprise Linux 4 clusters to the management interface to fail was fixed.
- A bug that caused updating existing fence devices to fail in some circumstances was fixed.
- A bug that caused the ricci storage module to fail to read mdadm device information was fixed.

This update adds the following enhancements:

- Support for configuration of LPAR fencing.
- Support for configuring NFS locking workarounds for cluster services.
- Support for choosing between the Xen and KVM hypervisors for virtual machine services.

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

1.23. coreutils

1.23.1. RHBA-2009:1262: bug fix update

An updated coreutils package that fixes several bugs and adds various enhancements is now available.

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

This updated package fixes the following bugs:

- previously, it was not possible to compile coreutils without SELinux support. This has been fixed so that removing the "--enable-selinux" option from the spec file allows coreutils to compile successfully. (BZ#488730)
- the "join" utility, which joins two text files, or a file and standard input, on a line-by-line basis, could experience a segmentation fault when running under a multibyte locale. In addition, multibyte locales could cause "join" to produce unexpected results. With this updated package, these coding errors have been corrected so that "join" completes correctly and successfully when run under a multibyte locale. (BZ#497368)
- the "df" utility reports the disk usage of a directory within a file system. Using "df" on a directory which contained autofs mount points under it did not cause autofs to mount those directories, which resulted in "df" not factoring in the disk usage of those automount directories. With this update, invoking the "df" command does trigger automount, which in turn results in a correct disk usage count. (BZ#497830)
- several other utilities in the coreutils package possessed undocumented options, which could have led to user confusion. Those undocumented options have been removed from their respective utilities, thus reducing the possibility for confusion. (BZ#468030)
- the "chmod", "chown" and "chgrp" commands all take the following options, which have the same effect: "-f", "--silent" and "--quiet". These flags cause the command to suppress most error messages. However, calling the command with one of these options on a non-existent file caued the command to output the

following message: "No such file or directory". These options now suppress error messages when called on non-existent files. (BZ#474220)

- the tail(1) man page contained a formatting error and a typo, both of which have been rectified. (BZ#470788)
- the rm(1) man page stated that the "rm" command possessed a "--directory" ('-d') option, whose purpose was to allow the removal of directories, including non-empty directories. However, invoking "rm --directory [dir]" always resulted in the following error message: "rm: cannot remove `some_dir': Is a directory". The rm(1) man page has been corrected and no longer lists "--directory" as an option. The recommended switch for recursively removing a directory and its contents is "--recursive" ('-r'). (BZ#473472)
- the coreutils package's locale directories were not owned by the coreutils package. This has been corrected by ensuring that all locale directories are owned by the package. (BZ#481804)

In addition, this updated package provides the following enhancements:

- the '-v' option of the "ls" command sorts directory listings based upon version numbers. However, "ls -v" did not sort vmlinuz-[version] files from the /boot/ directory in the correct order. This updated coreutils package enhances both "ls -v" and "sort -V" so that they are now able to sort /boot/vmlinuz-[version] files correctly. (BZ#253817)
- the "install" command now supports the "--compare" ('-c') flag, which causes "install" to compare each pair of source and destination files and, if the destination file's content is identical to the source (and disregarding any discrepancy between the owner, group, permissions and possibly SELinux context) then the destination file is not modified and the modification time is left unchanged. (BZ#453447)
- the "cp" and "mv" utilities now support the preservation of extended attributes on files and directories. In addition, Access Control Lists (ACLs) are now preserved when copying or moving files (with "cp" or "mv") to or from NFSv4-mounted file systems. (BZ#454072)

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

1.24. cpio

1.24.1. RHBA-2009:0379: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0379

An updated cpio package that fixes various bugs is now available.

GNU cpio copies files into or out of a cpio or Tar archive.

This updated cpio package includes fixes for the following bugs:

- when called with the "--pass-through" ('-p') option, which enables copy-pass mode, cpio did not always set the permissions of copied directories correctly. In certain circumstances, cpio always created directories with a permissions mode of 700 and did not respect the system umask. With this updated package, cpio copies directories while honoring the umask setting when using copy-pass mode, which resolves the issue.

- cpio was unable to write to a file on a remote system when using the "-O [archive]" option along with "--rsh-command". With this update, cpio is once again able to write files to remote systems. Note that the default remote shell is defined as /usr/bin/rsh.

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

1.25. cpuspeed

1.25.1. RHBA-2009:0424: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0424

An updated cpuspeed package that fixes various bugs is now available.

The cpuspeed package provides CPU frequency scaling support.

This updated package fixes the following bugs:

- the cpuspeed init script loaded the speedstep-centrino driver on Intel systems, even when the acpi-cpufreq driver had already loaded successfully. With both these drivers loaded, the system would not handle P-states correctly. The cpuspeed init script now attempts to load the speedstep-centrino driver only as a fallback for situations where it has not been able to load the acpi-cpufreq driver. Intel systems that can use the acpi-cpufreq driver no longer load the speedstep-centrino driver, and now handle P-states correctly. (BZ#485480)

- a development version of this package attempted to make cpuspeed run reliably on Xen kernels by only allowing cpuspeed to start on Xen kernels if the number of virtual CPUs in dom0 equalled the number of physical CPUs in the system. However, this condition can never be true until xend starts, and xend starts after cpuspeed. Therefore, cpuspeed would only run properly on Xen kernels if cpuspeed were restarted after the system completed the boot process. The restriction that cpuspeed can only start if the number of virtual and physical kernels are equal has therefore been removed, allowing cpuspeed to start on Xen kernels even when xend has not yet started. (BZ#488924 , BZ#498406 , BZ#492139)

1.26. crash

1.26.1. RHBA-2009:0049: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0049

Updated crash packages are now available.

Crash is a self-contained tool that can be used to investigate live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.

This updated package includes the following bug fix:

- The bt command displays a task's kernel-stack backtrace. When running this command against an x86 Xen kernel vmcore, crash did not correctly handle the transition from the IRQ stack back to the process stack, leading to a segmentation fault. The version of crash provided with this advisory contains a patch that corrects this issue, allowing users to analyze a vmcore file from a system with an x86 Xen kernel.

All users of crash should upgrade to this updated package.

1.26.2. RHBA-2009:1283: bug fix update

Updated crash packages that resolve several issues are now available.

The crash packages are used to investigate live systems and kernel core dumps created from the netdump, diskdump and kdump facilities.

These updated crash packages are rebased to upstream version 4.0-8.9 (BZ#494028) and provide fixes for the following bugs:

- if entered alone on the command line, the "set" command would cause a segmentation violation, because there is no concept of a "context" in the Xen hypervisor. Crash now prompts the user to provide an option with "set", and provides more meaningful error messages if the option selected is not applicable. (BZ#462819)

- crash would indicate "irq: invalid structure size: gate_struct" and dump a stack trace leading to x86_64_display_idt_table() when the "irq -d" option was run on AMD64 and Intel 64 Xen kernels. Now it will indicate that the -d option is not applicable. (BZ#464116)

- the "bt" command did not work correctly when running against the Xen hypervisor binary. The "bt -o" option, and setting it to run by default with "bt -O", would fail with the vmlinux-specific error message "bt: invalid structure size: desc_struct" with a stack trace leading to read_idt_table(). Now, it will display the generic error message "bt: -o option not supported or applicable on this architecture or kernel". The "bt -e" or "bt -E" will also display the same error message, as opposed to the command usage message. Lastly, the "bt -R" option would cause a segmentation violation; it has been fixed to work as it was designed. (BZ#464288)

- when run on a Xen hypervisor in which the backtrace leads to either "process_softirqs" or "page_fault", the "bt" command backtrace would indicate: "bt: cannot resolve stack trace". The recovery code would then terminate the command with the nonsensical error message: "bt: invalid structure size: task_struct". The command now properly terminates the backtrace. (BZ#474712 , BZ#466724)

- when run against the Xen hypervisor where the number of physical cpus outnumber the MAX_VIRT_CPUS value for the processor type, the "bt -a" command would fail after displaying backtraces for the first 32 (MAX_VIRT_CPUS) pcpus with the the error message: "bt: invalid vcpu". The command now shows backtraces for all pcpus. (BZ#471790)

- the "mod -[sS]" command would fail with the error message: "mod: cannot find or load object file for <name> module" if the target module object filename contains both underscore and dash characters. Crash now parses these filenames correctly. (BZ#480136)

- an existing Itanium INIT and MCA handler bug incorrectly writes the pseudo task's command name in its comm[] name string such that the CPU number may not be part of the string. The "bt" command could not link back to a PID 0 swapper task that was interrupted by an Itanium INIT or MCA exception, and displayed the error message: "bt: unwind: failed to locate return link (ip=0x0)!" Crash now uses a different method to obtain the CPU number for the interrupted task, and the backtrace correctly transitions back to the interrupted task. (BZ#487429)

- the starting backtrace location of active, non-crashing, xen dom0 tasks are not available in kdump dumpfiles, nor is there anything that can be searched for in their respective stacks. Therefore, for these tasks, the "bt" command would show either an empty backtrace or an invalid backtrace starting at the last

location where schedule() had been called. Instead, the "bt" command now provides an error message for these tasks that indicated "bt: starting backtrace locations of the active (non-crashing) xen tasks cannot be determined: try -t or -T options". (BZ#495586)

- Running the "bt" command against an x86 Xen kernel vmcore, the transition from the IRQ stack back to the process stack led to a segmentation fault. (BZ#478904)

The upstream changelog referenced below details additional bug fixes and enhancements provided by the rebase of this package.

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

1.27. cryptsetup-luks

1.27.1. RHBA-2009:1349: bug fix update

Updated cryptsetup-luks packages that fix various bugs are now available.

The cryptsetup-luks packages provide a utility for setting up encrypted devices using Device Mapper and the dm-crypt target.

This update provides the following bug fixes:

- the cryptsetup luksFormat command now properly wipes old filesystem signatures. (BZ#468910)
- the exit code for cryptsetup status command is no longer incorrect. (BZ#439191)
- the cryptsetup password entry message now includes the device name for which the user is being prompted. (BZ#437261)

All users of cryptsetup-luks should upgrade to these updated packages, which resolve these issues.

1.28. cscope

1.28.1. RHSA-2009:1102: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1102

An updated cscope package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

cscope is a mature, ncurses-based, C source-code tree browsing tool.

Multiple buffer overflow flaws were found in cscope. An attacker could create a specially crafted source code file that could cause cscope to crash or, possibly, execute arbitrary code when browsed with cscope. (CVE-2004-2541, CVE-2009-0148)

All users of cscope are advised to upgrade to this updated package, which contains backported patches to fix these issues. All running instances of cscope must be restarted for this update to take effect.

1.29. cups

1.29.1. RHBA-2009:1360: bug fix update

Updated cups packages that fix several bugs are now available.

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

These updated packages address the following bugs:

- the libcups library's HTTP state machine could get into a busy loop when a connection was closed at an unexpected point. (BZ#474323)
- web interface template files and translated template files were not marked as configuration files so local modifications to them would be lost when applying updates. This update will also cause local modifications to those files to be lost, but will prevent the same situation occurring with future updates. (BZ#474769)
- the "compression" job option was encoded with the wrong IPP tag, preventing the "document-format" job option from overriding automatic MIME type detection of compressed job files . (BZ#474814)
- the "mailto" CUPS notifier used the wrong line ending when transferring messages to an SMTP server, causing it not to send any notifications. (BZ#474920)
- automatic MIME type detection would fail when the document name was required by the relevant rule but only one file was present in the job. MIME detection would also fail with some rules using "+" (e.g. application/x-shell). (BZ#479635)
- incorrect web interface URLs would be given when the server's domain name resolved to a local loopback address on the server. (BZ#479809)
- the CUPS configuration file directive "Satisfy Any" was not correctly implemented, causing access to be restricted in situations where it should not have been. (BZ#481303)
- an optimization in the libcups library for fetching details of a print queue when its name is known caused problems with obtaining the name of the default printer when "lpoptions" files listed a non-existent queue as the default. (BZ#481481)
- RPM verification would fail on configuration files even though content changes were expected. (BZ#487161)
- the CUPS scheduler requires an updated version of the krb5 package in order to function correctly but this was not an RPM dependency. (BZ#489714)
- the text-only filter would not send form-feed characters correctly. (BZ#491190)
- incorrect IPP-Get-Jobs requests, accepted by CUPS in current versions of Red Hat Enterprise Linux but rejected in newer versions of the upstream package, were generated by the cupsGetJobs2() API function and by the lpstat and lpq commands. (BZ#497529)

All cups users should upgrade to these updated packages, which resolve these issues.

1.29.2. RHSA-2009:1082: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1082

Updated cups packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Common UNIX® Printing System (CUPS) provides a portable printing layer for UNIX operating systems. The Internet Printing Protocol (IPP) allows users to print and manage printing-related tasks over a network.

A NULL pointer dereference flaw was found in the CUPS IPP routine, used for processing incoming IPP requests for the CUPS scheduler. An attacker could use this flaw to send specially-crafted IPP requests that would crash the cupsd daemon. (CVE-2009-0949)

Red Hat would like to thank Anibal Sacco from Core Security Technologies for reporting this issue.

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

1.29.3. RHSA-2009:0429: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0429

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

This update has been rated as having important security impact by the Red Hat Security Response Team.

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

Multiple integer overflow flaws were found in the CUPS JBIG2 decoder. An attacker could create a malicious PDF file that would cause CUPS to crash or, potentially, execute arbitrary code as the "lp" user if the file was printed. (CVE-2009-0147, CVE-2009-1179)

Multiple buffer overflow flaws were found in the CUPS JBIG2 decoder. An attacker could create a malicious PDF file that would cause CUPS to crash or, potentially, execute arbitrary code as the "lp" user if the file was printed. (CVE-2009-0146, CVE-2009-1182)

Multiple flaws were found in the CUPS JBIG2 decoder that could lead to the freeing of arbitrary memory. An attacker could create a malicious PDF file that would cause CUPS to crash or, potentially, execute arbitrary code as the "lp" user if the file was printed. (CVE-2009-0166, CVE-2009-1180)

Multiple input validation flaws were found in the CUPS JBIG2 decoder. An attacker could create a malicious PDF file that would cause CUPS to crash or, potentially, execute arbitrary code as the "lp" user if the file was printed. (CVE-2009-0800)

An integer overflow flaw, leading to a heap-based buffer overflow, was discovered in the Tagged Image File Format (TIFF) decoding routines used by the CUPS image-converting filters, "imagetops" and "imagetoraster". An attacker could create a malicious TIFF file that could, potentially, execute arbitrary code as the "lp" user if the file was printed. (CVE-2009-0163)

Multiple denial of service flaws were found in the CUPS JBIG2 decoder. An attacker could create a malicious PDF file that would cause CUPS to crash when printed. (CVE-2009-0799, CVE-2009-1181, CVE-2009-1183)

Red Hat would like to thank Aaron Sigel, Braden Thomas and Drew Yao of the Apple Product Security team, and Will Dormann of the CERT/CC for responsibly reporting these flaws.

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

1.30. curl

1.30.1. RHSA-2009:1209: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1209

Updated curl packages that fix security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity.

Scott Cantor reported that cURL is affected by the previously published "null prefix attack", caused by incorrect handling of NULL characters in X.509 certificates. If an attacker is able to get a carefully-crafted certificate signed by a trusted Certificate Authority, the attacker could use the certificate during a man-in-the-middle attack and potentially confuse cURL into accepting it by mistake. (CVE-2009-2417)

cURL users should upgrade to these updated packages, which contain a backported patch to correct these issues. All running applications using libcurl must be restarted for the update to take effect.

1.30.2. RHSA-2009:0341: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0341

Updated curl packages that fix a security issue are now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity.

David Kierznowski discovered a flaw in libcurl where it would not differentiate between different target URLs when handling automatic redirects. This caused libcurl to follow any new URL that it understood, including the "file://" URL type. This could allow a remote server to force a local libcurl-using application to read a local file instead of the remote one, possibly exposing local files that were not meant to be exposed. (CVE-2009-0037)

Note: Applications using libcurl that are expected to follow redirects to "file://" protocol must now explicitly call curl_easy_setopt(3) and set the newly introduced CURLOPT_REDIR_PROTOCOLS option as required.

cURL users should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications using libcurl must be restarted for the update to take effect.

1.31. cvs

1.31.1. RHBA-2009:1370: bug fix update

An updated CVS package that fixes two bugs is now available.

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

This updated package fixes the following two bugs:

- mismatches between hosts sometimes caused the CVS client to present incorrect credentials to servers with gserver authentication. This update ensures the correct credentials are supplied by confirming the IP address of the currently-connected server so that host mismatch does not occur. (BZ#473245)
- attempting to process large numbers of files with long names caused problems with some scripts due to lengthy command line arguments. This problem has been resolved by adding the possibility of passing arguments through standard input. (BZ#462062)

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

1.32. cyrus-imapd

1.32.1. RHSA-2009:1116: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1116

Updated cyrus-imapd packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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

It was discovered that the Cyrus SASL library (cyrus-sasl) does not always reliably terminate output from the sasl_encode64() function used by programs using this library. The Cyrus IMAP server (cyrus-imapd) relied on this function's output being properly terminated. Under certain conditions, improperly terminated output from sasl_encode64() could, potentially, cause cyrus-imapd to crash, disclose portions of its memory, or lead to SASL authentication failures. (CVE-2009-0688)

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

1.32.2. RHBA-2009:1120: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1120

Updated cyrus-imapd packages that fix several bugs are now available.

The cyrus-imapd package contains a high-performance mail server with IMAP, POP3, NNTP and SIEVE support.

These updated cyrus-imapd packages provide fixes for the following bugs:

- attempting to connect to the update server failed and resulted in the following error messages being logged to /var/log/maillog:

  ```
  connect(192.168.11.110) failed: Invalid argument
  couldn't connect to MUPDATE server
  [IP address]: no connection to server
  FATAL: error connecting with MUPDATE server
  ```

  These updated packages correct this problem so that connecting to the update server now works as expected. (BZ#326511)

- on systems with 64-bit architectures, cyrus-imapd experienced a segmentation fault when replication was enabled. (BZ#484377)

In addition, these updated cyrus-imapd packages provide the following enhancement:

- more detailed information has been added to the ctl_cyrusdb(8) man page, which explains how to perform operations common to Cyrus databases. (BZ#463230)

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

1.33. cyrus-sasl

1.33.1. RHBA-2009:1330: bug fix update

Updated cyrus-sasl packages that fix various bugs are now available.

The cyrus-sasl packages contain the Cyrus implementation of SASL. SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols.

This errata fixes the following bugs:

- the shadow authentication method was not working properly on 64 bit architectures. The saslauthd might randomly crash if it was configured to authenticate against the shadow file. (BZ#433583)

- the rimap authentication method was not working properly when user passwords contain double quote characters. The saslauthd process would hang when it was configured to authenticate with the rimap method and user password contained such characters. (BZ#438533)
- the saslauthd init script did not support a reload command although it was mentioned in the init script usage instructions. The reload is now implemented as a conditional restart of the saslauthd daemon. (BZ#448154)
- the pluginviewer command did not display plugins which were not statically linked into it. The pluginviewer command is now linked dynamically so it can display any cyrus-sasl plugins which are installed on the system. (BZ#473197)
- the ldap authentication method had very long timeout for network failure detection. The saslauthd now sets a network failure timeout based on the ldap_timeout configuration option. (BZ#475726)

All Cyrus users are advised to install this updated package, which addresses these issues.

1.34. db4

1.34.1. RHBA-2009:0390: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0390

Updated db4 packages that resolve an issue are now available.

The Berkeley Database (Berkeley DB) is a programmatic toolkit that provides embedded database support for both traditional and client/server applications.

- These updated db4 packages fix a bug which, in certain circumstances, could have caused database environment recovery to fail.

All users of db4 are advised to upgrade to these updated packages, which resolve this issue.

1.35. device-mapper

1.35.1. RHBA-2009:1392: bug-fix and enhancement update

Updated device-mapper packages that include various bug fixes and enhancements are now available.

The device-mapper packages provide a library required by logical volume management utilities such as LVM2 and dmraid.

This update applies the following bug fixes:

- Fixes crash when dmsetup -U, -G, and -M options are used.
- Enforces device name length and character limitations.

This update adds the following enhancements:

- Adds "all" field to "-o fields" option, expanding to all fields of report type. That is, you can add -o <field_name> to specify which fields to print in certain commands; "-o all" expands to all possible fields known to report.
- Library now exports dm_tree_node_size_changed function and correctly propagates table size change up the device tree.
- Prints warning message if application releases the library and a memory pool is still in use (indicating a possible memory leak).
- Library is now compiled from merged device-mapper LVM2 tree (device-mapper library is now part of LVM2 source code tree).

All users of device-mapper should upgrade to these updated packages, which resolve these issues and include these enhancements.

1.36. device-mapper-multipath

1.36.1. RHBA-2009:0432: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0432

Updated device-mapper-multipath packages that resolve an issue are now available.

The device-mapper multipath packages provide tools to manage multipath devices by issuing instructions to the device-mapper multipath kernel module, and by managing the creation and removal of partitions for device-mapper devices.

These updated device-mapper-multipath packages fix the following bug:

- there was a race condition in the shutdown code for multipathd wherein a lock could be destroyed before all threads were finished using it. This could cause the machine to become unresponsive on multipathd shutdown. The multipathd daemon now waits for all threads to finish using the lock before destroying it, thus removing the race and resolving the issue.
- when adding a new multipath-capable block device, a race condition existed between the multipathd daemon and udev to multipath the new device. If udev--through multipath--updated the multipath devices first, then the multipathd daemon would not use the device-specific configurations for the device when it started monitoring the path. With this update, multipathd now correctly configures the device, even when udev notices it first, thus resolving the issue.

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

1.36.2. RHSA-2009:0411: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0411

Updated device-mapper-multipath packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The device-mapper multipath packages provide tools to manage multipath devices by issuing instructions to the device-mapper multipath kernel module, and by managing the creation and removal of partitions for device-mapper devices.

It was discovered that the multipathd daemon set incorrect permissions on the socket used to communicate with command line clients. An unprivileged, local user could use this flaw to send commands to multipathd, resulting in access disruptions to storage devices accessible via multiple paths and, possibly, file system corruption on these devices. (CVE-2009-0115)

Users of device-mapper-multipath are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. The multipathd service must be restarted for the changes to take effect.

Important: the version of the multipathd daemon in Red Hat Enterprise Linux 5 has a known issue which may cause a machine to become unresponsive when the multipathd service is stopped. This issue is tracked in the Bugzilla bug #494582; a link is provided in the References section of this erratum. Until this issue is resolved, we recommend restarting the multipathd service by issuing the following commands in sequence:

killall -KILL multipathd

service multipathd restart

1.36.3. RHBA-2009:0283: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0283

Updated device-mapper-multipath packages that fix a bug are now available.

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

- multipath must be able to open a file descriptor for each path that it monitors, plus 32 other file descriptors. By default, multipath can open 1024 file descriptors, which is sufficient for it to monitor 992 paths. If multipath is not able to open all the file descriptors that it needs, the multipath daemon will not function correctly, and in Red Hat Enterprise Linux 5.3, this situation exposes a kernel memory leak that can cause a system to stop responding. Previously, multipath would not warn users that it could not open enough file descriptors. Now, when multipath runs out of file descriptors, it prints an error message. System administrators can allow multipath to open more file descriptors by setting "max_fds" in the multipath.conf file to a sufficiently high number, or by setting "max_fds" to "max" to allow multipath to open as many file descriptors as the system allows.

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

1.36.4. RHEA-2009:1377: bug-fix and enhancement update

Updated device-mapper-multipath packages that fix several bugs and add various enhancements are now available.

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

This update applies the following bug fixes:

- Occasionally multipathd was ignoring a device's hardware type when configuring it after a path was added.
- Multiple documentation errors were fixed.
- Multipathd would occasionally hang or crash while shutting down.
- Multipath would always return a failure exit code when removing a device with multipath -f/-F.
- Multipathd wouldn't free its resources when it failed to execute a callout.
- Multipathd would always return a success exit code for interactive commands, even if the command failed or was invalid.
- The mpath_prio_alua pritority callout was failing on some setups because a buffer was too small.
- Multipathd was holding mount points in the /etc directory busy, even after they were unmounted.
- Multipath and multipathd were racing to create the mulitpath devices for newly added block devices. This was causing device creation to take a long time on some systems, and could even cause devices to have incorrect configurations.

This update adds the following enhancements:

- Default configurations were added for the Compellent Storage Center and the IBM DS3200, DS3300, DS4700, and DS5000.
- It is now possible to set the verbosity level for the multipath and multipathd commands in /etc/multipath.conf.
- The TUR path checker retries on more transient errors, so that multipathd will not fail a path due to a transient error.
- There is a new priority callout mpath_prio_intel to support the Intel Modular Server.
- There is now a multipath.conf.5 man page that explains the /etc/multipath.conf configuration file.

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

1.37. dhcp

1.37.1. RHBA-2009:1331: bug fix update

A dhcp update that fixes several bugs is now available.

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. The dhcp package provides a relay agent and ISC DHCP service required to enable and administer DHCP on a network.

This update applies the following updates:

- Supplying an interface name (on the command line) that was longer than the size declared by the IFNAMSIZ macro caused an unexpected segmentation fault. This update contains an added process that properly checks the validity of interface names, which resolves this issue. (BZ#441524)
- This update corrects a bug in the way the dhclient-script file processed the $localClockFudge variable. In previous releases, this bug caused the NTPD daemon to restart unexpectedly at times. (BZ#450301)
- dhclient now retains relay agent options when it enters the INIT and REBIND states. (BZ#450545)
- A bug in the network shutdown code prevented dhclient from correctly honoring the PEERNTP and PEERDNS variables in /etc/sysconfig/network-scripts/ifcfg-* files. This caused dhcp to replace a modified /etc/ntp.conf file with a default version during a network service restart. This update fixes the bug, ensuring that dhclient-script no longer replaces the /etc/ntp.conf file upon network service restart if PEERNTP and PEERDNS are both set to 'yes'. (BZ#471543)
- The dhcpd and dhcrelay init scripts do not support the 'try-restart' and 'reload' arguments. In previous releases, however, using these arguments did not output any error messages to inform the user that the restart/reload attempt failed. With this release, using the unsupported 'try-restart' or 'reload' arguments with the dhcpd or dhcrelay init scripts will correctly display the usage screen and exit the script with a status code 3. (BZ#491868)

Users of dhcp are advised to apply this update.

1.38. dhcpv6

1.38.1. RHBA-2009:1409: bug fix update

Updated dhcpv6 packages that resolve an issue are now available.

The dhcpv6 packages implement the Dynamic Host Configuration Protocol (DHCP) for Internet Protocol version 6 (IPv6) networks, in accordance with RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). DHCP is a protocol that allows individual devices on an IP network to get their own network configuration information. It consists of: dhcp6c(8), the DHCPv6 client daemon; dhcp6s(8), the DHCPv6 server daemon; and dhcp6r(8), the DHCPv6 relay agent.

Previously, DHCPv6 was not able to be chosen as the IPv6 configuration method in anaconda. Choosing DHCPv6 instead of the default 'Automatic neighbor discovery' may have caused the installer to crash, returning a stack trace to the terminal. With this update, the libdhcp6client library code has been updated, and DHCPv6 can now be chosen as the IPv6 configuration method in the installer, which resolves this issue. (BZ#506722)

All users of dhcpv6 are advised to upgrade to these updated packages, which resolve this issue.

1.39. dmidecode

1.39.1. RHBA-2009:1324: enhancement update

An updated dmidecode package that fixes a bug and adds enhancements is now available.

The dmidecode package provides utilities for extracting x86 and ia64 hardware information from the system BIOS or EFI, according to the SMBIOS/DMI standard. This information typically includes system manufacturer, model name, serial number, BIOS version, asset tag as well as a lot of other details of varying level of interest and reliability depending on the manufacturer.

This will often include usage status for the CPU sockets, expansion slots (e.g. AGP, PCI, ISA) and memory module slots, and the list of I/O ports (e.g. serial, parallel, USB).

This updated package adds the following enhancement:

- the previous version of the dmidecode package was based on upstream version 2.7 and lacked support for a variety of newer hardware. The package now provides version 2.9, which:
  - updates support for SMBIOS specification version 2.5
  - decodes slot IDs of AGP 8x and PCIE slots
  - decodes newer processor characteristics (multi-core, multi-thread, 64-bit)
  - supports newer types of chassis, processor, socket, connector and memory device
  - supports x86 EFI

  (BZ#459048)

This updated package fixes the following bug:

- the default method used by dmidecode to retrieve entries from the DMI table produces unaligned access errors when used on Itanium systems. When built for the Itanium architecture, this version of the package includes a workaround that avoids these errors. (BZ#459048).

Users of dmidecode are advised to upgrade to this updated package, which adds this enhancements and fixes this bug.

1.40. dmraid

1.40.1. RHBA-2009:1347: bug-fix and enhancement update

Updated dmraid packages that fix several bugs and add enhancements are now available.

The dmraid packages contain the ATARAID/DDF1 activation tool that supports RAID device discovery, RAID set activation, and displays properties for ATARAID/DDF1 formatted RAID sets on Linux kernels using device-mapper.

This update applies the following bug fixes:

- The dmraid logwatch-based email reporting feature has been moved from the dmraid-events package into the new dmraid-events-logwatch package. Consequently, systems that use this dmraid feature need to complete the following manual procedure: 1. Ensure the new 'dmraid-events-logwatch' package is installed. 2. Un-comment the functional portion of the "/etc/cron.d/dmeventd-logwatch" crontab file.
- The sgpio and dmevent_tool applications get installed with the dmraid package now.
- The drive order for isw RAID01 sets is now identical with the OROM order.
- Various issues with wrong LED rebuild and metadata states have been fixed.

This update adds the following enhancements:

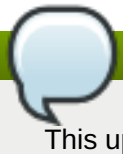
- Device Failure Monitoring, using the tools dmraid and dmevent_tool, is now included in Red Hat Enterprise Linux 5.4 as a Technology Preview. Device Failure Monitoring provides the ability to watch and report device failures on component devices of RAID sets.
- dmraid now automatically activates device event monitoring for the isw metadata format (Intel IMSM). The dmevent_tool is still available to allow for manual (de)registration.

- dmraid now supports an "--rm_partitions" option to allow for removing partition devices for RAID set component devices.
- Activation of isw RAID sets on disks with long serial numbers is now supported.

All dmraid users should upgrade to these updated packages, which resolve these issues and add these enhancements.

1.41. dos2unix

1.41.1. RHBA-2009:0276: bug fix update



Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0276

Updated dos2unix packages that resolve two bugs are now available.

The dos2unix utility converts DOS or MAC format text files to UNIX format.

This updated package provides fixes for the following bugs:

- dos2unix did not allow for instances where a user specified the -c option without a conversion mode name following it. An input in this format would therefore result in a segmentation fault. Dos2unix now exits safely with a message to the user that option -c requires an argument.
- when dos2unix created a new file as the output of its conversion (when run with the -n option), the new file would always have its permission mode set as 600, regardless of the permission mode of the original file. Dos2unix now sets the permission mode for the new file to be the same as the mode of the old file, filtered through the user's umask.

Users of dos2unix should upgrade to this updated package, which resolves these issues.

1.42. dump

1.42.1. RHBA-2009:0425: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0425

Updated dump packages that resolve several issues are now available.

The dump package contains both dump and restore commands. The dump command examines files in a file system, determines which ones need to be backed up, and copies those files to a specified disk, tape, or other storage medium. The restore command performs the inverse function of dump; it can restore a full backup of a file system. Subsequent incremental backups can then be layered on top of the full backup. Single files and directory subtrees may also be restored from full or partial backups.

These updated dump packages provide fixes for the following bugs:

- when running the dump command without specifying a dump level, then neither did dump's output indicate the dump level, as in the following example output:

```
DUMP: Date of this level  dump: Thu Apr  2 09:05:09 2009
DUMP: Date of this level  dump: Thu Apr  2 09:05:09 2009
```

  This has been corrected in these updated packages so that the dump level is no longer missing in output in which it is shown.

- When the dump command was called without a default dump level specified on the command line, then the dump level defaulted to 0, while the dump(8) man page stated that the default level was 9. The actual default dump level that is used when this is not specified in arguments to dump is 0, and the man page has been changed to reflect this.

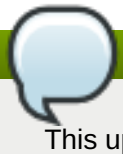
- the restore(8) man page, as well as the program's help information, incorrectly implied that the '-P [file]' option could be used in conjunction with the '-A [archive_file]', which is not the case. Attempting to use both options results in the following error message: "restore: A option is not valid for P command". The restore(8) man page and restore's help has been corrected so that it is clear that the '-A' and '-P' options cannot be used together.

- several typos in the dump(8) man page were corrected.

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

1.43. dvd+rw-tools

1.43.1. RHBA-2009:1072: bug fix update



Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1072

An updated dvd+rw-tools package that addresses a bug and corrects a typo is now available for Red Hat Enterprise Linux 5.

The dvd+rw-tools package is a collection of tools to master DVD+RW/+R media.

- on some systems with manually-operated DVD drive trays (ie drives that cannot be closed mechanically, such as most slim-line drive trays), burning data to DVD media would produce an erroneous "Error writing to disk" alert. The data was, in fact, successfully burnt to the DVD and the newly burnt DVD was then ejected. The inability of the drive tray to close mechanically, however, caused dvd+rw-tools to return an "unable to reload tray" message which, in turn, caused the 'writing to disk' error to present. With this update, dvd+rw-tools treats the underlying "START_STOP_UNIT" message properly and, consequently, the misleading alert does not present. (BZ#390961)

- a typo in the dvd+rw-tools.spec file was corrected. The "%{dist}" tag on the "Release" line was corrected to "%{?dist}". The correction ensures an rpm can be built from the dvd+rw-tools source even if a distribution is not defined in either the Makefile or your local ~/.rpmmacros file. (BZ#440621)

All dvd+rw-tools users should upgrade to this updated package, which resolves these issues.

1.44. e2fsprogs

1.44.1. RHBA-2009:1291: bug fix and enhancement update

An updated e2fsprogs package that fixes various bugs and adds an enhancement is now available.

The e2fsprogs package contains a number of utilities that create, check, modify, and correct inconsistencies in second extended (ext2) file systems. e2fsprogs contains e2fsck (which repairs file system inconsistencies after an unclean shutdown), 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.

This updated version of e2fsprogs addresses the following issues:

- when mke2fs or resize2fs was run on a device of exactly 2^32 file system blocks (16 terabytes for 4 kilobit blocks), these commands would fail with a "File too large" error, because the maximum file system size was 2^32-1 blocks. mke2fs and resize2fs now round down by one block to allow the commands to succeed for devices of exactly 2^32 blocks, and the error no longer presents. (BZ#241285)
- the German localization of an e2fsprogs process contained a typographical error. This has been corrected and the correct line now displays. (BZ#488960)
- the e2fsck method, pass3, would use a pointer regardless of whether it contained a null value. This would result in a segfault. The method has been corrected and the problem no longer presents. (BZ#505110)
- the ismounted method was set to use two arguments when it required three. This has been corrected, and the method now works as expected. (BZ#505110)
- the debugfs method, logdump, performed a call to fclose without checking that the value being passed was not null. This would result in segfault. The method now checks for a null before attempting to pass the value, and does not call fclose if a null is present. (BZ#505110)
- a typographical error in the uuidd initscript that caused an incorrect status to me set has been corrected. (BZ#506080)

The updated package also includes the following enhancement:

- running mke2fs on devices larger than 8 terabytes required the "-F" (force) option to succeed. This update removes that requirement. (BZ#241285)

All users should upgrade to this updated package, which resolves the listed issues and adds the noted enhancement.

1.45. e4fsprogs

1.45.1. RHBA-2009:1413: bug fix update

An updated e4fsprogs package that fixes a bug is now available.

The e4fsprogs package contains a number of utilities for creating, checking, modifying, and correcting inconsistencies in ext4 and ext4dev file systems. e4fsprogs contains e4fsck (used to repair file system inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 file system), tune4fs (used to modify file system parameters), and most other core ext4fs file system utilities.

Important

this package is now designed and intended to be installed alongside the original e2fsprogs package in Red Hat Enterprise Linux. As such, certain binaries in the e4fsprogs package have been given new names. For example, the utility that checks ext4 file systems for consistency has been renamed to "e4fsck", thus allowing the original "e2fsck" program from the e2fsprogs package to coexist on the same system. (BZ#485316)

Notably, this updated e4fsprogs package includes a fix for the following bug:

- invoking the "stats" command while at the "debuge4fs" prompt could cause "debuge4fs" to segmentation fault due to a missing check to see whether the file system was currently open. This has been fixed in this updated package so that calling "stats" is now safe. (BZ#482894)

All users of e4fsprogs are advised to upgrade to this updated package, which resolves this issue.

1.46. ecryptfs-utils

1.46.1. RHSA-2009:1307: Low security, bug fix, and enhancement update

Updated ecryptfs-utils packages that fix a security issue, various bugs, and add enhancements are now available for Red Hat Enterprise Linux 5.

This update has been rated as having low security impact by the Red Hat Security Response Team.

eCryptfs is a stacked, cryptographic file system, transparent to the underlying file system and provides per-file granularity.

eCryptfs is released as a Technology Preview for Red Hat Enterprise Linux 5.4. These updated ecryptfs-utils packages have been upgraded to upstream version 75, which provides a number of bug fixes and enhancements over the previous version. In addition, these packages provide a graphical program to help configure and use eCryptfs. To start this program, run the command:

ecryptfs-mount-helper-gui

Important: the syntax of certain eCryptfs mount options has changed. Users who were previously using the initial Technology Preview release of ecryptfs-utils are advised to refer to the ecryptfs(7) man page, and to update any affected mount scripts and /etc/fstab entries for eCryptfs file systems.

A disclosure flaw was found in the way the "ecryptfs-setup-private" script passed passphrases to the "ecryptfs-wrap-passphrase" and "ecryptfs-add-passphrase" commands as command line arguments. A local user could obtain the passphrases of other users who were running the script from the process listing. (CVE-2008-5188)

These updated packages provide various enhancements, including a mount helper and supporting libraries to perform key management and mounting functions.

Notable enhancements include:

- a new package, ecryptfs-utils-gui, has been added to this update. This package depends on the pygtk2 and pygtk2-libglade packages and provides the eCryptfs Mount Helper GUI program. To install the GUI, first install encryptfs-utils and then issue the following command:

```
yum install ecryptfs-utils-gui
```

(BZ#500997)

- the "ecryptfs-rewrite-file" utility is now more intelligent when dealing with non-existent files and with filtering special files such as the "." directory. In addition, the progress output from "ecryptfs-rewrite-file" has been improved and is now more explicit about the success status of each target. (BZ#500813)
- descriptions of the "verbose" flag and the "verbosity=[x]" option, where [x] is either 0 or 1, were missing from a number of eCryptfs manual pages, and have been added. Refer to the eCryptfs man pages for important information regarding using the verbose and/or verbosity options. (BZ#470444)

These updated packages also fix the following bugs:

- mounting a directory using the eCryptfs mount helper with an RSA key that was too small did not allow the eCryptfs mount helper to encrypt the entire key. When this situation occurred, the mount helper did not display an error message alerting the user to the fact that the key size was too small, possibly leading to corrupted files. The eCryptfs mount helper now refuses RSA keys which are to small to encrypt the eCryptfs key. (BZ#499175)
- when standard input was redirected from /dev/null or was unavailable, attempting to mount a directory with the eCryptfs mount helper caused it to become unresponsive and eventually crash, or an "invalid value" error message, depending on if the "--verbosity=[value]" option was provided as an argument, and, if so, its value. With these updated packages, attempting to mount a directory using "mount.ecryptfs" under the same conditions results in either the mount helper attempting to use default values (if "verbosity=0" is supplied), or an "invalid value" error message (instead of the mount helper hanging) if standard input is redirected and "--verbosity=1" is supplied, or that option is omitted entirely. (BZ#499367)
- attempting to use the eCryptfs mount helper with an OpenSSL key when the keyring did not contain enough space for the key resulted in an unhelpful error message. The user is now alerted when this situation occurs. (BZ#501460)
- the eCryptfs mount helper no longer fails upon receiving an incorrect or empty answer to "yes/no" questions. (BZ#466210)

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

1.47. efax

1.47.1. RHBA-2009:1113: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1113

An updated efax package that fixes a bug is now available.

The efax program is a small ANSI C/POSIX utility that sends and receives faxes using any Class 1, 2 or 2.0 fax modem.

This updated efax package fixes a bug which caused a segmentation fault when attempting to send a fax due to the incorrect use of an internal efax function.

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

1.48. esc

1.48.1. RHBA-2009:1310: bug fix update

An updated esc package that fixes various bugs is now available.

The esc package contains the "Smart Card Manager" GUI tool, which allows the user to manage security smart cards. The primary function of the tool is to enroll smart cards, so that they can be used for common cryptographic operations, such as secure email and website access.

This updated package fixes the following bugs:

- If a smart card were inserted when the esc daemon was already running then there could be odd behaviors when the ESC GUI was opened. For example, if the smart card was blank, then the Phone Home configuration dialog would not open. When the smart card was removed, then esc could crash. (BZ#496410)
- If a user attempted to re-enroll a formatted token when the RE_ENROLL value was set to NO, then the ESC wrongly gave an error that the token was suspended, not that re-enrollment wasn't allowed. This message has been corrected. (BZ#494981)

This update also includes enhancements for smart card management:

- Certificate System previously supported re-enrollment for tokens, which allows a formatted token to be re-formatted with new certificates. This enhancement also allows smart cards to have renewal operations, so existing certificates can have renewed.
- This release includes enhancements to streamline the security officer mode for ESC. Security officer mode allows designated users to perform in-person token enrollments, as added security. This simplifies launching the ESC GUI in security officer mode.

Users of esc are advised to upgrade to this updated package, which resolves these issues.

1.49. ethtool

1.49.1. RHEA-2009:1408: enhancement update

An enhanced ethtool package that adds support for GRO options is now available.

Ethtool allows querying and changing of ethernet card settings, such as speed, port, autonegotiation, and PCI locations.

This updated package adds the following enhancement:

- generic receive offload (GRO) has been added to some network drivers in Red Hat Enterprise Linux 5.4. GRO aggregates packets before they're processed by the rest of the stack. This allows TCP performance to be greatly enhanced at high speeds. In particular, it's crucial for good 10GbE performance. With GRO enabled, you should observe higher throughput, lower CPU utilization of network traffic, or both; especially with smaller message sizes.

  The kernel in Red Hat Enterprise Linux 5.4 allows users to manually control whether GRO is enabled for supported ethernet adapters. This updated ethtool provides a command-line interface -- "ethtool -k" -- for setting and querying that flag. (BZ#509398)

All ethtool users should upgrade to this updated package which adds this capability.

1.50. evince

1.50.1. RHBA-2009:1404: bug fix update

An updated evince package that fixes a printing bug is now available.

evince is a GNOME-based document viewer.

This update fixes a flaw in evince versions prior to 0.6.0-8 discovered by Jonathan Peatfield:

- when printing "n" copies of a non-postscript document, "n times n" copies were printed instead. (That is, if two copies were requested, four copies -- 2 x 2 -- were printed.) This flaw has been corrected. Note: the underlying cause of this problem also influenced collated printing, reversed printing and printing of sets of pages. (BZ#439937)

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

1.51. evolution

1.51.1. RHBA-2009:1260: bug fix update

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

Evolution is the GNOME collection of personal information management (PIM) tools.

These updated evolution packages provide fixes for the following bugs:

- when adding a new Exchange account, a Mailbox name separate from the user name can now be specified. (BZ#205787)
- pasting text into an event summary by issuing the Ctrl+V control code did not work as expected. (BZ#208356)
- running Evolution in a different language caused it to not display certain translations such as "On This Computer", "Personal" and specific calendar and address book names. (BZ#210858)
- when attempting to import a certificate from the Edit Preferences -> Certificates menu, the subsequent Trust dialog box appeared below the file selector window, forcing users to manually move both windows in order to accomplish the task. (BZ#212206)
- Evolution crashed due to a segmentation fault when reading certain email messages when accessibility was enabled. (BZ#212481)
- attempting to import a vCard File containing contacts into a new address book created during the import process failed, and no contacts were imported. All contacts imported in this way are now present in the new address book. (BZ#215470)
- selecting the "On This Computer" folder and then clicking Folder -> Properties produced no result. The "Properties" menu item is now correctly grayed-out. (BZ#215479)
- Evolution did not honor the selected day when adding a memo while in calendar view: the user had to manually alter the memo's date afterward. (BZ#217541)
- searching an address book using the "any field" option when no results were found caused Evolution to display all contacts instead of none. This behavior is now more intuitive: no contacts are displayed when none are found. (BZ#217714)

- while in Mail view, deselecting a previously-selected group of messages by clicking on one of those selected did not result in that message being shown in the preview pane. (BZ#227710)
- when accessibility was enabled, specific combinations of calender-viewing actions caused Evolution to crash. (BZ#428817)
- when starting Evolution for the first time with a German (de_DE) locale, the setup wizard window was too large for some monitors to display. (BZ#432322)
- dragging-and-dropping messages into the "Personal Folders" caused those messages to be irretrievably lost. Dropping messages into "Personal Folders" is now disallowed. (BZ#437768)
- Evolution's account editor did not strip whitespace characters in hostnames, which caused a failure to connect when attempting to retrieve email. (BZ#446945)
- sorting email by subject did not always result in the expected alphabetical sorting. (BZ#449797)
- the Contact Quick-Add window allowed users to click "OK" without selecting an address book, which did not result in the contact being added to any address book. (BZ#449983)
- attempting to download Exchange messages for offline use caused Evolution to segmentation fault. Evolution no longer crashes, and downloading Exchange messages works as expected, allowing for offline use. (BZ#472872)
- it was not possible to create a new folder from the New Search Folder dialog box and related menus. Also, attempting to name a new folder and then clicking the "Create" button caused Evolution to crash under certain circumstances. (BZ#473024)
- moving an Exchange folder containing subfolders to a different location resulted in the loss of all subfolders and their emails. With this update, all subfolders and their contents are copied or moved correctly and without any loss of data. (BZ#480849)

In addition, these updated packages provide the following enhancements:

- improved support for CalDAV. (BZ#484252)
- the cursor now conveniently moves to the new rule when it is created in the "Add Rule" dialog box. (BZ#218539)

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

1.52. evolution-connector

1.52.1. RHBA-2009:1261: bug fix update

An updated evolution-connector package that fixes various bugs is now available.

The evolution-connector package is an add-on to Evolution, an e-mail, calendar and information management client, that gives it the ability to interact with a Microsoft® Exchange Server.

This updated evolution-connector package includes fixes for the following bugs:

- when adding a new Exchange account, a Mailbox name separate from the user name can now be specified. (BZ#205787)
- a memory leak related to using Exchange accounts has been plugged. (BZ#393761)

- dragging-and-dropping messages into the "Personal Folders" caused those messages to be irretrievably lost. Dropping messages into "Personal Folders" is now disallowed. (BZ#437768)
- incoming mail filters had no effect on messages received by Exchange-based email accounts. This has been fixed in this updated package so that incoming mail filters work as expected with Exchange accounts. (BZ#446095)
- in certain situations, notifications were not shown for calendar events stored on an Exchange Server. With this updated package, notifications work correctly as long as Evolution is configured to remember Exchange Server passwords. Otherwise, notifications fail to be shown. (BZ#480164)
- moving an Exchange folder containing subfolders to a different location resulted in the loss of all subfolders and their emails. With this update, all subfolders and their contents are copied or moved correctly and without any loss of data. (BZ#480849)

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

1.53. evolution-data-server

1.53.1. RHSA-2009:0354: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0354

Updated evolution-data-server and evolution28-evolution-data-server packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Evolution Data Server 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 multiple other applications.

Evolution Data Server did not properly check the Secure/Multipurpose Internet Mail Extensions (S/MIME) signatures used for public key encryption and signing of e-mail messages. An attacker could use this flaw to spoof a signature by modifying the text of the e-mail message displayed to the user. (CVE-2009-0547)

It was discovered that Evolution Data Server did not properly validate NTLM (NT LAN Manager) authentication challenge packets. A malicious server using NTLM authentication could cause an application using Evolution Data Server to disclose portions of its memory or crash during user authentication. (CVE-2009-0582)

Multiple integer overflow flaws which could cause heap-based buffer overflows were found in the Base64 encoding routines used by Evolution Data Server. This could cause an application using Evolution Data Server to crash, or, possibly, execute an arbitrary code when large untrusted data blocks were Base64-encoded. (CVE-2009-0587)

All users of evolution-data-server and evolution28-evolution-data-server are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of Evolution Data Server and applications using it (such as Evolution) must be restarted for the update to take effect.

1.53.2. RHBA-2009:1259: bug fix update

Updated evolution-data-server packages that resolve several issues are 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 multiple other applications.

These updated evolution-data-server packages provide fixes for the following bugs:

- occasionally, a "?" appeared as the last result of the list obtained when viewing the "Select Contacts from Address Book" dialog. With these updated packages, this incorrect entry no longer occurs in the dialog window when selecting contacts. (BZ#220431)
- The IMAP mail protocol distinguishes between messages which are "new" on the server and messages which are "new" for a mail client. This dichotomy led Evolution Data Server to only apply filters to one of the "new" groups and not to the other, which meant that email filters were not applied to certain messages With these updated packages, filters now apply to all IMAP messages which are new for the client, with the result that all messages can now be successfully filtered. (BZ#247779)
- when attempting to connect to an Exchange 2007 server, the server's response sometimes caused Evolution to segmentation fault. Although the possibility of an Exchange 2007 server's response causing Evolution to crash has been fixed with these updated packages, it is still not possible for Evolution to communicate successfully with an Exchange 2007 server. (BZ#433648)
- when Evolution was configured with two IMAP accounts, deleting one of those accounts could have caused Evolution to segmentation fault. These updated packages fix a variable referencing error with the result that disabling a mail account no longer causes Evolution to crash. (BZ#437758)
- Evolution Data Server could segmentation fault when provided a malformed CalDAV calendar URL. With these updated packages, Evolution performs better error-checking on calendar URLs, which prevents this issue from occurring. (BZ#440232)
- the Exchange connector for Evolution Data Server contained several memory leaks which have been plugged in these updated packages. (BZ#460669)
- when adding a new Exchange account, a Mailbox name separate from the user name can now be specified. (BZ#460671)
- when reading a calendar via the CalDAV protocol, Evolution failed to correctly adjust the time of events based on timezone information. (BZ#462007)
- improved support for CalDAV. (BZ#484232)
- attempting to download Exchange messages for offline use caused Evolution to segmentation fault. Evolution no longer crashes, and downloading Exchange messages works as expected, allowing for offline use. (BZ#489869)
- Evolution incorrectly switched to Daylight Saving Time (DST) one week later than the time when DST should have started. With these updated packages, DST now takes effect at the correct time. (BZ#490218)
- Evolution did not provide notifications for events located on a foreign Exchange calendar. This update ensures that Evolution is able to notify based on foreign Exchange calendar events in the same way as for local calendars. (BZ#494847)

All users of evolution-data-server are advised to upgrade to these updated packages, which resolve these issues.

1.54. file

1.54.1. RHBA-2009:0456: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0456

An updated file package that fixes a bug is now available.

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

This updated file package provides fixes for the following bug:

- A core file, which is created when a program crashes, contains the name of the crashed program. The file command did not report the correct program name on some core files. The file command reports the correct name with this updated package.

Users are advised to upgrade to this updated file package, which resolves this issue.

1.55. findutils

1.55.1. RHEA-2009:1410: enhancement update

An enhanced findutils package is now available.

The findutils package contains programs for locating files. The find utility searches for files matching a certain set of criteria. The xargs utility builds and executes command lines from standard input arguments.

This updated findutils package adds the following enhancement:

- when using the "find" utility to search a directory hierarchy which contained autofs mounts, it dutifully triggered the aufofs mounts so that they could be searched, even when "find" had been directed to exclude NFS shares. With these updated packages, "find" possesses an additional exclusionary flag, "-xautofs", that prevents "find" from searching all autofs direct mounts in the searched directory hierarchy. (BZ#485672)

Users of findutils are advised to upgrade to this updated package, which adds this enhancement.

1.56. fipscheck

1.56.1. RHEA-2009:1266: enhancement update

An updated fipscheck package which contains enhancements necessary for FIPS validation is 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.

These updated fipscheck packages add the following enhancements:

- previously, the fipscheck libraries and binaries were installed in / (root). However, because they are not required by anything in /, they are now relocated to /usr. (BZ#475800)

- previously, the fipscheck libraries were packaged in the main fipscheck package. This would lead to a file conflict when installing fipscheck on architectures with multilib support. The fipscheck libraries are now shipped in fipscheck-lib subpackages for each architecture, therefore avoiding the file conflict. (BZ#502676)
- fipscheck now includes a runtime integrity self-test which is necessary for FIPS 140-2 level 1 validation of Red Hat Enterprise Linux 5 cryptography modules.
- the FIPSCHECK_DEBUG environment variable adds improved debugging. Error messages can be saved to the syslog or sent to stderr.
- fipscheck can now compute HMACs on multiple files at the same time.

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

1.57. firefox

1.57.1. RHSA-2009:1162: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1162

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

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

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 as the user running Firefox. (CVE-2009-2462, CVE-2009-2463, CVE-2009-2464, CVE-2009-2465, CVE-2009-2466, CVE-2009-2467, CVE-2009-2469, CVE-2009-2471)

Several flaws were found in the way Firefox handles malformed JavaScript code. A website containing malicious content could launch a cross-site scripting (XSS) attack or execute arbitrary JavaScript with the permissions of another website. (CVE-2009-2472)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.0.12. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.12, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.57.2. RHSA-2009:1095: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1095

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

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

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 as the user running Firefox. (CVE-2009-1392, CVE-2009-1832, CVE-2009-1833, CVE-2009-1837, CVE-2009-1838, CVE-2009-1841)

Multiple flaws were found in the processing of malformed, local file content. If a user loaded malicious, local content via the file:// URL, it was possible for that content to access other local data. (CVE-2009-1835, CVE-2009-1839)

A script, privilege elevation flaw was found in the way Firefox loaded XML User Interface Language (XUL) scripts. Firefox and certain add-ons could load malicious content when certain policy checks did not happen. (CVE-2009-1840)

A flaw was found in the way Firefox displayed certain Unicode characters in International Domain Names (IDN). If an IDN contained invalid characters, they may have been displayed as spaces, making it appear to the user that they were visiting a trusted site. (CVE-2009-1834)

A flaw was found in the way Firefox handled error responses returned from proxy servers. If an attacker is able to conduct a man-in-the-middle attack against a Firefox instance that is using a proxy server, they may be able to steal sensitive information from the site the user is visiting. (CVE-2009-1836)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.0.11. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.11, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.57.3. RHSA-2009:0449: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0449

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

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

A flaw was found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code as the user running Firefox. (CVE-2009-1313)

For technical details regarding this flaw, refer to the Mozilla security advisory for Firefox 3.0.10. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.10, which corrects this issue. After installing the update, Firefox must be restarted for the change to take effect.

1.57.4. RHSA-2009:0436: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0436

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

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

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 as the user running Firefox. (CVE-2009-1302, CVE-2009-1303, CVE-2009-1304, CVE-2009-1305)

Several flaws were found in the way malformed web content was processed. A web page containing malicious content could execute arbitrary JavaScript in the context of the site, possibly presenting misleading data to a user, or stealing sensitive information such as login credentials. (CVE-2009-0652, CVE-2009-1306, CVE-2009-1307, CVE-2009-1308, CVE-2009-1309, CVE-2009-1310, CVE-2009-1312)

A flaw was found in the way Firefox saved certain web pages to a local file. If a user saved the inner frame of a web page containing POST data, the POST data could be revealed to the inner frame, possibly surrendering sensitive information such as login credentials. (CVE-2009-1311)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.0.9. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.9, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.57.5. RHSA-2009:0397: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0397

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

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

A memory corruption flaw was discovered in the way Firefox handles XML files containing an XSLT transform. A remote attacker could use this flaw to crash Firefox or, potentially, execute arbitrary code as the user running Firefox. (CVE-2009-1169)

A flaw was discovered in the way Firefox handles certain XUL garbage collection events. A remote attacker could use this flaw to crash Firefox or, potentially, execute arbitrary code as the user running Firefox. (CVE-2009-1044)

For technical details regarding these flaws, refer to the Mozilla security advisories. You can find a link to the Mozilla advisories in the References section of this errata.

Firefox users should upgrade to these updated packages, which resolve these issues. For Red Hat Enterprise Linux 4, they contain backported patches to the firefox package. For Red Hat Enterprise Linux 5, they contain backported patches to the xulrunner packages. After installing the update, Firefox must be restarted for the changes to take effect.

1.57.6. RHSA-2009:0315: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0315

An updated firefox package that fixes various security issues is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Mozilla Firefox is an open source Web browser.

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 as the user running Firefox. (CVE-2009-0040, CVE-2009-0771, CVE-2009-0772, CVE-2009-0773, CVE-2009-0774, CVE-2009-0775)

Several flaws were found in the way malformed content was processed. A website containing specially-crafted content could, potentially, trick a Firefox user into surrendering sensitive information. (CVE-2009-0776, CVE-2009-0777)

For technical details regarding these flaws, please see the Mozilla security advisories for Firefox 3.0.7. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.7, and which correct these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.57.7. RHSA-2009:0256: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0256

An updated firefox package that fixes various security issues is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Mozilla Firefox is an open source Web browser.

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 as the user running Firefox. (CVE-2009-0352, CVE-2009-0353, CVE-2009-0356)

Several flaws were found in the way malformed content was processed. A website containing specially-crafted content could, potentially, trick a Firefox user into surrendering sensitive information. (CVE-2009-0354, CVE-2009-0355)

A flaw was found in the way Firefox treated HTTPOnly cookies. An attacker able to execute arbitrary JavaScript on a target site using HTTPOnly cookies may be able to use this flaw to steal the cookie. (CVE-2009-0357)

A flaw was found in the way Firefox treated certain HTTP page caching directives. A local attacker could steal the contents of sensitive pages which the page author did not intend to be cached. (CVE-2009-0358)

For technical details regarding these flaws, please see the Mozilla security advisories for Firefox 3.0.6. You can find a link to the Mozilla advisories in the References section.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.6, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.58. flash-plugin

1.58.1. RHSA-2009:1188: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1188

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

Multiple security flaws were found in the way Flash Player displayed certain SWF content. An attacker could use these flaws to create a specially-crafted SWF file that would cause flash-plugin to crash or, possibly, execute arbitrary code when the victim loaded a page containing the specially-crafted SWF content. (CVE-2009-1862, CVE-2009-1863, CVE-2009-1864, CVE-2009-1865, CVE-2009-1866, CVE-2009-1868, CVE-

2009-1869)

A clickjacking flaw was discovered in Flash Player. A specially-crafted SWF file could trick a user into unintentionally or mistakenly clicking a link or a dialog. (CVE-2009-1867)

A flaw was found in the Flash Player local sandbox. A specially-crafted SWF file could cause information disclosure when it was saved to the hard drive. (CVE-2009-1870)

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.0.32.18.

1.58.2. RHSA-2009:0332: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0332

An updated Adobe Flash Player package that fixes several security issues is now available for Red Hat Enterprise Linux 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

Multiple input validation flaws were found in the way Flash Player displayed certain SWF (Shockwave Flash) content. An attacker could use these flaws to create a specially-crafted SWF file that could cause flash-plugin to crash, or, possibly, execute arbitrary code when the victim loaded a page containing the specially-crafted SWF content. (CVE-2009-0520, CVE-2009-0519)

It was discovered that Adobe Flash Player had an insecure RPATH (runtime library search path) set in the ELF (Executable and Linking Format) header. A local user with write access to the directory pointed to by RPATH could use this flaw to execute arbitrary code with the privileges of the user running Adobe Flash Player. (CVE-2009-0521)

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.0.22.87.

1.59. foomatic

1.59.1. RHBA-2009:1240: bug fix update

An updated foomatic package that fixes two bugs is now available.

Foomatic is a comprehensive, spooler-independent database of printers, printer drivers, and driver descriptions. An interactive version of this database is available at http://www.linuxfoundation.org/en/OpenPrinting/Database/DatabaseIntro

Foomatic provides utilities to generate driver description files and printer queues for CUPS, LPD, LPRng, and PDQ from the database. As well, foomatic makes it possible to read PJL-options out of PJL-capable laser printers and take them into account when driver description files are generated.

The package also includes spooler-independent command line interfaces to manipulate queues (foomatic-configure) and to print files and manipulate print jobs (foomatic printjob).

This updated package addresses the following issues:

- previously, PostScript Printer Descriptions (PPDs) created for printers for which no page margin information was available used ImageableArea settings that equated to zero-width margins (ie, foomatic over-optimistically assumed edge-to-edge printing capability in the absence of specific information to the contrary). With this update, PPDs created for printers with no included margin information are set to 127mm (36 points or 0.5") by default. This avoids problems with print jobs being cropped at the edges of the page. (BZ#244348)

- spooler auto-detection is not part of foomatic and, previously, foomatic did not set a default spooler. Consequently, the foomatic-configure command failed to detect that CUPS was present if a default spooler was not set in /etc/foomatic/defaultspooler (which was not created by default during foomatic installation). With this update, /etc/foomatic/defaultspooler is created during installation and the default spooler is set to CUPS, ensuring foomatic-configure is aware of CUPS. (BZ#454684)

All foomatic users should upgrade to this updated package, which resolves these issues.

1.60. freetype

1.60.1. RHSA-2009:1061: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1061

Updated freetype packages that fix various security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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.

Tavis Ormandy of the Google Security Team discovered several integer overflow flaws in the FreeType 2 font engine. If a user loaded a carefully-crafted font file with an application linked against FreeType 2, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2009-0946)

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.

1.61. gcc

1.61.1. RHBA-2009:1376: bug fix update

A gcc update that resolves several GFortran compiler bugs (along with several other bugs) is now available.

The gcc packages include C, C++, Java, Fortran, Objective C, and Ada 95 GNU compilers, along with related support libraries.

This update applies the following bug fixes:

- 64-bit multiplication by constant on the x86 platform caused unexpected aborts when compiling code that used 'unsigned long long' variables. This was because the compiler did not check whether

CONST_DOUBLE_LOW was positive when multiplying constants. With this update, the compiler now check if CONST_DOUBLE_LOW is positive, ensuring that 'unsigned long long' variables are processed correctly during compiles. (BZ#465807)

- A bug in the way the GFortran compiler processed unique symtrees could have prevented some valid GFortran code from compiling if the code contained symbols defined by USE and ONLY clauses. Whenever this occurred, the compile attempt would fail with a segmentation fault. This update adds a special function that correctly reconciles symbols with unique symtrees, which resolves this bug. (BZ#483845)
- Using the -fabi-version=1 option prevented some valid C++ code from compiling. This was because Version 1 of the C++ ABI did not properly substitute template parameters. This release corrects this behavior, adding a function that correctly sets the processing_template_decl to 0 when performing substitutions. (BZ#492011)
- A bug in the way gcc optimized code could have prevented some samples of valid C code from compiling (resulting in an internal compiler error) whenever the -O1 option was used. This was because during optimized compiles, the C compiler did not properly process bounds; this resulted in incorrect computations for loop iterations. With this update, the compiler now processes bounds correctly, ensuring that valid C code compiles correctly with the -O1 option set. (BZ#490513)
- The GFortran compiler did not handle FMT= character array arguments properly. This prevented some samples of valid GFortran code from compiling; whenever this occurred, the compile attempt would fail with a segmentation fault. This update adds new functions to correct how FMT= character array arguments are handled, thereby resolving this bug. (BZ#492209)
- The expand_expr_real_1() function of the C compiler did not handle TRUTH_ANDIF_EXPR and TRUTH_ORIF_EXPR cases correctly. As a result, a compile attempt could fail with an internal compiler error on the PowerPC platform. This update applies an upstream fix for this issue. (BZ#495469)

Users are advised to upgrade to this gcc update, which applies these fixes.

1.62. gcc44

1.62.1. RHBA-2009:1375: bug fix and enhancement update

The GNU Compiler Collection (GCC) version 4.4.0 is now available as Technology Preview.

The gcc44 packages provide the GNU Compiler Collection (GCC), which includes GNU compilers and related support libraries for C, C++, and Fortran programming languages. These packages also include libgomp, the GNU implementation of the OpenMP Application Programming Interface for multi-platform shared-memory parallel programming.

These new gcc43 packages provide a snapshot release of GCC version 4.4.0 as a Technology Preview. The libgomp version included in this release supports OpenMP version 3.0, a backward-compatible update to the OpenMP 2-series. (BZ#494563)

This release also features the following bug fixes:

- GFortran provided improper DWARF definitions for array parameters (i.e. missing upper bounds). This was caused by a bug in gcc/fortran/trans-decl.c that provided incorrect debugging information for variable-length, non-desc Fortran arrays. With this release, Gfortran now provides proper DWARF definitions for arrays parameters. (BZ#459374)
- A bug in GFortran made it possible for an internal compiler error to incorrectly escalate to a segmentation fault (instead of terminating the compilation gracefully). An upstream fix for this bug is now included with this release. (BZ#466928)

- Whenever gcc is used with the option -march=z9-ec or -march=z10, hardware decimal floating point (DFP) support is used by default. (BZ#474367)
- An improper option (i.e. %global _use_internal_dependency_generator 0) used during the build of libgomp in previous releases disabled "file coloring". This caused RPM to erroneously detect a file conflict on /usr/lib/libgomp.so.1.0.0 when installing libgomp from the Itanium compatibility layer. This release includes a properly-built libgomp, which resolves this issue. (BZ#503725)

Note

the -fgnu89-inline option instructs GCC to use traditional GNU semantics for inline functions when in C99 mode. In this Technology Preview, -fgnu89-inline is used by default. This is necessary because the Red Hat Enterprise Linux 5 header files expect GNU inline semantics instead of ISO C99 semantics. Further, these header files have not been adjusted to request inline settings through attributes. (BZ#493929)

All users interested in testing gcc44 as a Technology Preview are advised to install these packages. Note that this release replaces the gcc43 Technology Preview packages provided in previous releases.

1.63. gdb

1.63.1. RHBA-2009:1361: bug fix update

A gdb update that fixes several bugs and improves gfortran debugging is now available.

The GNU Project debugger (normally referred to as GDB) debugs programs written in C, C++, and other languages by executing them in a controlled fashion, and then printing out their data.

This update applies the following bug fixes:

- Normally, static variables always have the same debugging information for each possible constructor/destructor implementation kind, which allows the compiler to keep their DIE (debugging information entry) only in the single abstract instance of the constructor. However, GDB did not automatically inherit whole DIEs from the abstract instances to the concrete instances. As such, the static variables in C++ constructors were not visible from GDB. With this update, GDB now inherits whole DIEs to ensure that static variables do not become inaccessible. (BZ#445912)
- GDB now supports the use of 64-bit ELF files for 32-bit platforms (i.e. elf64-i386). (BZ#457187)
- It was possible for GDB to print an error when trying to access an allocatable or otherwise dynamic array or string variable in Fortran. This was because GDB did not account for the fact that the lower bound for Fortran arrays was 1 (rather than 0). This made it possible for array size calculations to result in invalid values (i.e. too high) when allocating unbound or dynamically-bound Fortran arrays. This release corrects the way GDB processes Fortran arrays; it also adds functions to verify the validity of a calculated array size first before attempting to allocate it. (BZ#459380)
- Variables imported from Fortran modules can be now accessed from GDB with the same scope as the program being debugged. (BZ#466118 , BZ #457793)
- Variables shared by Fortran "common blocks" can be now accessed from GDB with the same scope as the program being debugged. Further, common blocks valid in the current program scope can be printed using the GDB command 'info common'. (BZ#459762)

- Allocatable arrays, objects with assumed size, and pointers to objects can be now accessed from GDB in the same manner that they are accessed from the program being debugged. (BZ#460250 , BZ#459952 , BZ#465301 , BZ#505333)
- Variables of type 'logical (kind=8)' can be now accessed from GDB. (BZ#465310)
- For external references, GCC does not produce DWARF debug information. As a result, GDB could not access Thread Local Storage (TLS) variables from a local source file if those variables were defined in a different source file. This made it possible for certain memory addresses to become unaccessible to GDB. With this release, GDB can now process TLS variables using ELF structures instead of DWARF; as such, GDB can now access TLS variables regardless of where those variables were defined. (BZ#494412)
- Running gcore (or any 'attach' or 'detach' command sequence) on a multi-threaded process that was halted with 'kill -STOP' could unexpectedly resume some of that process's threads. This behavior was caused by a kernel bug (present in upstream version 2.6.29) that remained unfixed in Red Hat Enterprise Linux 5 kernels to maintain backward compatibility. While this update does not fix the kernel bug, it applies a GDB workaround that ensures threads from a halted multi-threaded process do not unexpectedly resume. (BZ#498595)

This update also implements various parts of Fortran language support. With this implementation, gfortran44 (not gfortran) is now used to compile Fortran programs. The gfortran44 compiler is provided by the gcc44 update (included in this release as a Technology Preview).

GDB users are advised to apply this update.

1.64. gdm

1.64.1. RHSA-2009:1364: Low security and bug fix update

Updated gdm packages that fix a security issue and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having low security impact by the Red Hat Security Response Team.

The GNOME Display Manager (GDM) is a configurable re-implementation of XDM, the X Display Manager. GDM allows you to log in to your system with the X Window System running, and supports running several different X sessions on your local machine at the same time.

A flaw was found in the way the gdm package was built. The gdm package was missing TCP wrappers support, which could result in an administrator believing they had access restrictions enabled when they did not. (CVE-2009-2697)

This update also fixes the following bugs:

- the GDM Reference Manual is now included with the gdm packages. The gdm-docs package installs this document in HTML format in "/usr/share/doc/". (BZ#196054)
- GDM appeared in English on systems using Telugu (te_IN). With this update, GDM has been localized in te_IN. (BZ#226931)
- the Ctrl+Alt+Backspace sequence resets the X server when in runlevel 5. In previous releases, however, repeated use of this sequence prevented GDM from starting the X server as part of the reset process. This was because GDM sometimes did not notice the X server shutdown properly and would subsequently fail to complete the reset process. This update contains an added check to explicitly notify GDM whenever the X server is terminated, ensuring that resets are executed reliably. (BZ#441971)

- the "gdm" user is now part of the "audio" group by default. This enables audio support at the login screen. (BZ#458331)
- the gui/modules/dwellmouselistener.c source code contained incorrect XInput code that prevented tablet devices from working properly. This update removes the errant code, ensuring that tablet devices work as expected. (BZ#473262)
- a bug in the XOpenDevice() function prevented the X server from starting whenever a device defined in "/etc/X11/xorg.conf" was not actually plugged in. This update wraps XOpenDevice() in the gdk_error_trap_pop() and gdk_error_trap_push() functions, which resolves this bug. This ensures that the X server can start properly even when devices defined in "/etc/X11/xorg.conf" are not plugged in. (BZ#474588)

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

1.65. gfs-kmod

1.65.1. RHBA-2009:1212: bug-fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1212

Updated gfs-kmod packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The gfs-kmod packages contain modules that provide the ability to mount and use GFS file systems.

This update applies the following bug fix:

- A bug which did not flush the journal after a fsync to a stuffed inode has been fixed.

All gfs-kmod users should upgrade to these updated packages, which resolve this issue.

1.65.2. RHBA-2009:1338: bug-fix update

Updated gfs-kmod packages which fix several bugs are now available.

The gfs-kmod packages contain kernel modules that provide the functionality to mount and use GFS file systems.

These updated packages apply the following bug fixes:

- A potential deadlock causing gfs to hang in 'wait_for_completion' was fixed by prefaulting buffer pages.
- Applications using sendfile on files with the inherit_jdata flag are now notified that sendfile will not work on those files instead of failing.
- A bug that could potentially cause a page allocation failure has been fixed.
- A bug that caused fsyncs to stuffed inodes fail to flush the journal has been fixed.

Users are advised to upgrade to these latest gfs-kmod packages, which resolve these issues.

1.66. gfs-utils

1.66.1. RHBA-2009:1336: bug fix update

Updated gfs-utils packages that fix various bugs are now available.

The gfs-utils packages provide the user-level tools necessary to mount and use GFS file systems.

These updated gfs-utils packages apply the following bug fixes:

- An issue was fixed which caused gfs_fsck to attempt to fix the wrong bitmap.
- gfs_fsck's ability to fix damaged resource groups has been improved.
- A human readable option has been added to to gfs_tool df.
- Fixed an issue which could potentially cause gfs_fsck to remove everything in a corrupt filesystem.
- gfs_grow performance has been improved on 1k block size filesystems.
- Fix a segfault in gfs_fsck when fixing a 'EA leaf block type' problem.
- The gfs service is no longer disabled after an upgrade.

All users of gfs-utils should upgrade to these updated packages, which resolve these issues.

1.67. gfs2-utils

1.67.1. RHBA-2009:0477: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0477

Updated gfs2-utils packages that fix a bug are now available.

The gfs2-utils packages provide the user-space tools necessary to mount, create, maintain, and test GFS2 file systems.

The updated gfs2-utils packages apply the following bug fix:

- A segfault was fixed in gfs2_fsck which can be triggered by a stuffed directory inode block also being listed as a data block.

All users of gfs2-utils should upgrade to these updated packages, which resolve this issue.

1.67.2. RHBA-2009:0418: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0418

Updated gfs2-utils packages that fix a bug are now available.

The gfs2-utils packages provide the user-space tools necessary to mount, create, maintain, and test GFS2 file systems.

The updated gfs2-utils packages apply the following bug fix:

- In certain cases a conversion between gfs1 and gfs2 filesystem could cause corruption; this bug has been fixed.

All users of gfs2-utils should upgrade to these updated packages, which resolve these issues.

1.67.3. RHBA-2009:0280: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0280

Updated gfs2-utils packages that fix various bugs are now available.

The gfs2-utils packages provide the user-space tools necessary to mount, create, maintain and test GFS2 file systems.

The updated gfs2-utils packages apply the following bug fixes:

- Other mount options will now be properly recognized when using 'noatime' or 'nodiratime'.
- gfs2_grow now works with block sizes other than 4k.

All users of gfs2-utils should upgrade to these updated packages, which resolve these issues.

1.67.4. RHSA-2009:1337: Low security and bug fix update

An updated gfs2-utils package that fixes multiple security issues and various bugs is now available for Red Hat Enterprise Linux 5.

This update has been rated as having low security impact by the Red Hat Security Response Team.

The gfs2-utils package provides the user-space tools necessary to mount, create, maintain, and test GFS2 file systems.

Multiple insecure temporary file use flaws were discovered in GFS2 user level utilities. A local attacker could use these flaws to overwrite an arbitrary file writable by a victim running those utilities (typically root) with the output of the utilities via a symbolic link attack. (CVE-2008-6552)

This update also fixes the following bugs:

- gfs2_fsck now properly detects and repairs problems with sequence numbers on GFS2 file systems.
- GFS2 user utilities now use the file system UUID.
- gfs2_grow now properly updates the file system size during operation.
- gfs2_fsck now returns the proper exit codes.
- gfs2_convert now properly frees blocks when removing free blocks up to height 2.

- the gfs2_fsck manual page has been renamed to fsck.gfs2 to match current standards.
- the 'gfs2_tool df' command now provides human-readable output.
- mounting GFS2 file systems with the noatime or noquota option now works properly.
- new capabilities have been added to the gfs2_edit tool to help in testing and debugging GFS and GFS2 issues.
- the 'gfs2_tool df' command no longer segfaults on file systems with a block size other than 4k.
- the gfs2_grow manual page no longer references the '-r' option, which has been removed.
- the 'gfs2_tool unfreeze' command no longer hangs during use.
- gfs2_convert no longer corrupts file systems when converting from GFS to GFS2.
- gfs2_fsck no longer segfaults when encountering a block which is listed as both a data and stuffed directory inode.
- gfs2_fsck can now fix file systems even if the journal is already locked for use.
- a GFS2 file system's metadata is now properly copied with 'gfs2_edit savemeta' and 'gfs2_edit restoremeta'.
- the gfs2_edit savemeta function now properly saves blocks of type 2.
- 'gfs2_convert -vy' now works properly on the PowerPC architecture.
- when mounting a GFS2 file system as '/', mount_gfs2 no longer fails after being unable to find the file system in '/proc/mounts'.
- gfs2_fsck no longer segfaults when fixing 'EA leaf block type' problems.

All gfs2-utils users should upgrade to this updated package, which resolves these issues.

1.68. ghostscript

1.68.1. RHSA-2009:0421: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0421

Updated ghostscript packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Ghostscript is a set of software that provides a PostScript interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files.

It was discovered that the Red Hat Security Advisory RHSA-2009:0345 did not address all possible integer overflow flaws in Ghostscript's International Color Consortium Format library (icclib). Using specially-crafted ICC profiles, an attacker could create a malicious PostScript or PDF file with embedded images that could

cause Ghostscript to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0792)

A buffer overflow flaw and multiple missing boundary checks were found in Ghostscript. An attacker could create a specially-crafted PostScript or PDF file that could cause Ghostscript to crash or, potentially, execute arbitrary code when opened. (CVE-2008-6679, CVE-2007-6725, CVE-2009-0196)

Red Hat would like to thank Alin Rad Pop of Secunia Research for responsibly reporting the CVE-2009-0196 flaw.

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

1.68.2. RHSA-2009:0345: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0345

Updated ghostscript packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Ghostscript is a set of software that provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files.

Multiple integer overflow flaws which could lead to heap-based buffer overflows, as well as multiple insufficient input validation flaws, were found in Ghostscript's International Color Consortium Format library (icclib). Using specially-crafted ICC profiles, an attacker could create a malicious PostScript or PDF file with embedded images which could cause Ghostscript to crash, or, potentially, execute arbitrary code when opened by the victim. (CVE-2009-0583, CVE-2009-0584)

All users of ghostscript are advised to upgrade to these updated packages, which contain a backported patch to correct these issues.

1.68.3. RHBA-2009:1257: bug fix update

A ghostscript update that fixes several bugs is now available.

The Ghostscript suite provides a PostScript(TM) 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.

This update applies the following fixes:

- an incorrect offset computation that occurred when handling subglyphs made it possible for ghostscript to read uninitialized data. When this occurred, ghostscript would crash with a segmentation fault. This update corrects the offset computation, preventing ghostscript from reading uninitialized data. (BZ#450717)

- the way that the Ghostscript source code used pointer aliasing could produce unexpected results when strict aliasing optimizations are in use. To avoid problems, this ghostscript update was built using the -fno-strict-aliasing option, which disables strict aliasing optimization. (BZ#465960)
- a typographical error in the gsiparam.h header file made it possible for some PDF files to cause ghostscript to fall into an infinite loop. This update fixes the error. (BZ#473889)
- the gdevpsu.c source file incorrectly defined the point size of A3 pages, which sometimes resulted in incorrect document page sizes. This update fixes the point size definition error , ensuring that A3 pages are always printed with the correct size. (BZ#480978)
- this update corrects how the cvrs PostScript operator performs sign extensions. This fix prevents range errors from occurring on 64-bit platforms. (BZ#488127)
- this update also fixes ColorSpace initialization in the InkJet Server (IJS) driver, which is used by hpijs and gimp-print drivers in some configurations. In previous releases, print jobs that did not initialize ColorSpace failed whenever they used Ghostscript to render and print PDFs on devices that used the ijs driver. (BZ#504254)

Users of ghostscript are advised to apply this update.

1.69. giflib

1.69.1. RHSA-2009:0444: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0444

Updated giflib packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The giflib packages contain a shared library of functions for loading and saving GIF image files. This library is API and ABI compatible with libungif, the library that supported uncompressed GIF image files while the Unisys LZW patent was in effect.

Several flaws were discovered in the way giflib decodes GIF images. An attacker could create a carefully crafted GIF image that could cause an application using giflib to crash or, possibly, execute arbitrary code when opened by a victim. (CVE-2005-2974, CVE-2005-3350)

All users of giflib are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. All running applications using giflib must be restarted for the update to take effect.

1.70. glib2

1.70.1. RHSA-2009:0336: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0336

Updated glib2 packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GLib is the 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.

Diego Pettenò discovered multiple integer overflows causing heap-based buffer overflows in GLib's Base64 encoding and decoding functions. An attacker could use these flaws to crash an application using GLib's Base64 functions to encode or decode large, untrusted inputs, or, possibly, execute arbitrary code as the user running the application. (CVE-2008-4316)

Note: No application shipped with Red Hat Enterprise Linux 5 uses the affected functions. Third-party applications may, however, be affected.

All users of glib2 should upgrade to these updated packages, which contain backported patches to resolve these issues.

1.71. glibc

1.71.1. RHBA-2009:1415: bug fix and enhancement update

Updated **glibc** packages that fix various bugs and implement a technology preview of per-thread memory pooling are now available.

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

This update applies the following bug fixes:

- A **strcmp()** call in the **setlocale()** function could cause a segmentation fault (**SIGSEGV**) to occur in multi-threaded applications. This was caused by an improper **free()** call, which freed **_nl_global_locale.__names[category]** around the same time **strcmp()** tried to access it. As such, it was possible for **strcmp()** to access **_nl_global_locale.__names[category]** after it was freed (i.e. no longer available), resulting in a segmentation fault. To fix this, this update adds a **return()** call to make **_nl_global_locale.__names[category]** available when **strcmp()** accesses it. (BZ#455580)

- The **getifaddrs()** function listed invalid IPv6 interface names for Infiniband devices. This was because Infiniband names are 20 bytes long, while **glibc** only prepares an 8-byte string array (i.e. **sll_addr**) for interface names. When **getifaddrs()** copied the 20-byte string into **sll_addr**, the result was a corrupted, invalid interface name. To prevent this, this update expands the field size from 8 bytes to 24 bytes, allowing **getifaddrs()** to copy 20-byte Infiniband names to the **sll_addr** string array. (BZ#463252)

- A previous update to **glibc** resulted in a performance regression with **mutex()** calls. This was caused by the addition of mutual exclusion (mutex) types tested by **pthread_mutex_lock()** and

pthread_mutex_unlock(). To alleviate the problem, this update optimizes the **pthread_mutex_lock()** and **pthread_mutex_unlock()** for the most common mutex types, which improves the performance of **mutex()** calls in most common user scenarios. (BZ#467316)

- **dl_runtime_profile** on the IBM System Z incorrectly used the instruction lr to remove stack frames, which could result in corrupted stacks in rare cases. With this update, **dl_runtime_profile** uses the correct instruction (**lgr**) to remove stack frames instead. (BZ#470300)

- An improper break statement in the **getgrouplist()** function caused searches to abort prematurely. This resulted in a bug that prevented **getgrouplist()** from retrieving group definitions from LDAP. As such, applications that used **getgrouplist()** to authenticate group details could not honor supplementary group credentials defined in LDAP. This update removes the improper break statement in **getgrouplist()**, enabling proper retrieval of group definitions from LDAP. (BZ#470768)

- The **/var/run/utmp** file keeps track of all log-ins and log-outs to the system. All attempts to open it with read-write permission are denied and audited. The **setutent_file()** function call always attempted to open the **/var/run/utmp** with read-write permissions, resulting in the audit system logging a large volume of denial records. With this update, **setutent_file()** now only attempts to open **/var/run/utmp** with read-only permissions, thereby reducing the volume of audited records. (BZ#475332)

- The **elf/dl-load.c** source file did not properly free allocated memory before **dlclose()** function calls. This made it possible for some **dlopen()** and **dlclose()** calls to result in a memory leak. This update corrects the **elf/dl-load.c** source file by instructing it to free all allocated memory, thereby preventing a memory leak whenever **dlopen()** or **dlclose()** are used. (BZ#476725) .

- The **getent** command no longer incorrectly uses a comma to delimit aliases when displaying network map entries. As such, running **getent networks** now only displays network map entries using spaces or tabs as delimiters. (BZ#484082)

- This update now includes the **RUSAGE_THREAD** definition in the **glibc** headers. This allows the **getrusage()** function call to retrieve information about the resource usage of a thread. (BZ#484214).

- The **inet6_opt_init()** function incorrectly counted the first octet when computing the length of extension headers (i.e. **extlen**). This was contrary to the definition of extension header lengths as per RFC 2460. With this update, **inet6_opt_init()** now subtracts 1 octet unit when computing for **extlen**. (BZ#488748)

- As per RFC3493, **getnameinfo()** should return **EAI_NONAME** when both **nodename** and **servname** variables are set to **NULL** while the **NI_NAMEREQD** flag is set. However, **getnameinfo()** returned **0** in this situation. This update adds an **if** statement to **getnameinfo()** to correct its behavior as per RHC3493. (BZ#489419).

- The **nscd paranoia** mode instructs **nscd** to restart periodically. However, whenever **nscd** attempted to restart itself in this mode, it incorrectly used the system call **execv("/proc/self/exe", argv)**. As a result, **nscd** would restart with an process name of **exe** instead of **nscd**. To correct this, the **nscd paranoia** mode now instructs **nscd** to restart using **readlink("/proc/self/exe", target, 255)**, which allows **nscd** to preserve its process name upon restart. Note that**nscd** will still use **execv("/proc/self/exe", argv)** if the attempt to use **readlink()** fails. (BZ#490010)

- The **sysconf()** function call used an obsolete **const** attribute. This caused the **gcc** compiler to incorrectly return **errno** when it attempted to compile code while using some optimization options. With this update, **sysconf()** no longer uses the obsolete **const**, ensuring that optimization works as expected at compile time. (BZ#490821)

- The **inet6_rth_reverse()** function produced an incorrect return order of addresses in the routing header. This was caused by an incorrect identifier (**ip6r0_segleft** instead of **ip6r0_len**) in the **inet/inet6_rth.c** source code. This update corrects the identifier, ensuring that **inet6_rth_reverse()** returns the correct output. (BZ#494849)

- The **inet6_rth_add()** function incorrectly returned **0** even when the routing header did not have enough space to store an address. This was caused by a lack of error checking routines to verify routing header size. This update applies an additional **if** statement to verify the routing header size. (BZ#494850).

- Previous versions of **glibc** coded **malloc()** in a way that was not thread-safe. This could have led to unexpected program crashes in some cases. This release revises the **malloc()** code to ensure better thread safety, as well as to adhere to C standards. (BZ#502901)

- This update removes an extra comma at the end of the **dlfcn.h** header file's enumerator list. This typographical error caused **dlfcn.h** to fail **g++** pedantic tests in previous releases. (BZ#504704)

- A bug in the **nptl/pthread_mutex_lock.c** code prevented **pthread_mutex** calls from honoring some types of private futex attributes. This update applies a patch that corrects this behavior, ensuring that **pthread_mutex** calls honor all types of private futex attributes for PI mutexes.(BZ#495955).

- Applications that performed a large number of directory reads ran much slower on 64-bit Red Hat Enterprise Linux 5 compared to 64-bit Red Hat Enterprise Linux 4. This was partly because while Red Hat Enterprise Linux 5 uses the system call **getdents()** to retrieve directory entries for both 32-bit and 64-bit platforms, Red Hat Enterprise Linux 4 used **getdents64()** for 64-bit platforms. Because of this, the **opendir()** function did not allocate more memory for directory reads on 64-bit platforms, resulting in much slower reads on Red Hat Enterprise Linux 5. To resolve this, **opendir()** now has an increased default buffer size; if memory allocation fails (as it would on 32-bit applications), it retries the memory allocation with a smaller buffer size. This improves the performance of directory reads on 64-bit platforms, while ensuring that **opendir()** still works on 32-bit platforms. (BZ#484440)

- An incorrect parameter in the **MALLOC_COPY()** function of the **libc/malloc/malloc.c** source file could supply an incorrect **size_t** value for **realloc()**. With this update, **MALLOC_COPY()** is now fixed, ensuring that it always supplies the correct **size_t** information for **realloc()**. (BZ#478499)

- With this update, users can now run **fork()** safely in one thread while a **pthread** stack cache updates in another thread. Doing so no longer causes the process created by **fork()** to crash. (BZ#477705)

- This update also applies several upstream fixes to **nscd**. These fixes prevent **nscd** from crashing due to segmentation faults in some cases. (BZ#464918 and 483636)

- This update also includes the ability to enable (and configure) per-thread memory pools. This capability enables higher scalability accross many sockets and cores, and is included in this release as a technology preview. The environmental variable **MALLOC_PER_THREAD=1** enables per-thread memory pools, while **MALLOC_ARENA_MAX** and **MALLOC_ARENA_TEST** control the amount of additional memory used for the memory pools (if any). **MALLOC_ARENA_MAX** sets a maximum number of memory pools used, regardless of the number of cores; **MALLOC_ARENA_TEST** specifies that the number of cores should be tested once it reaches a set value. Note that once per-thread memory pooling becomes fully supported, it will also become the default behavior; this will render the **MALLOC_PER_THREAD** option obsolete then. (BZ#494758)

Users are advised to upgrade to this version of **glibc**.

1.71.2. RHBA-2009:1202: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1202

Updated glibc packages that fix a bug are now available.

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

These updated glibc packages fix the following bug:

- previous versions of glibc coded the malloc() function in a way that was not thread-safe, which could have led to unexpected program crashes in some cases. With these updated packages, the malloc() code has been revised to ensure better thread safety, as well as to adhere to C standards. (BZ#502901)

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

1.72. gnome-python2-desktop

1.72.1. RHBA-2009:0405: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0405

An updated gnome-python2-desktop package that fixes a bug in the GNOME Keyring bindings is now available.

The gnome-python2-desktop package contains additional Python bindings for GNOME. It should be used together with gnome-python2.

This update fixes the following bug:

- The gnomekeyring.find_items_sync() function was returning a list of long integers representing the addresses of GnomeKeyringFound instances. These addresses are not useful in Python, however, and this update adds Python bindings for GnomeKeyringFound. IT also changes find_items_sync() to return a list of GnomeKeyringFound instances. (BZ#479280)

All gnome-python2-desktop users should install this update which addresses this issue.

1.73. gnome-session

1.73.1. RHBA-2009:1079: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1079

An updated gnome-session package that fixes a bug is now available.

gnome-session manages a GNOME desktop session. It starts up the other core GNOME components and handles logout and saving the session.

This updated gnome-session package fixes the following bug:

- gnome-session, also referred to as the GNOME Session Manager, remembers information such as which applications were open at the time of logout (among other session details), and restores these applications upon logging in again. A bug prevented gnome-session from restoring two applications when both of them were named the same, such as could happen with GKrellM system monitors, multiple instances of the KDE Konsole, and potentially other applications with multiple instances. With this updated package, gnome-session is able to restore all same-named application instances which were saved in the previous session, thus resolving the problem. (BZ#484431)

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

1.74. grep

1.74.1. RHBA-2009:0481: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0481

An updated grep package that fixes various bugs is now available.

Grep searches through textual input for lines matching a regular expression.

This updated grep package includes fixes for the following bugs:

- while searching certain immense binary files in which the newline character did not appear for large expanses (for hundreds of megabytes of text, for instance), grep may have missed a subsequent match. Because the grep utility is not intended to process arbitrarily-long files in this manner, this updated version now exits with a "line too long" error message and an appropriate error code under these conditions. (BZ#483073)
- when operating on particular multi-byte character sets (but not, notably, UTF-8), grep could enter an infinite loop and become unresponsive. This has been fixed in this updated package so that grep is once again able to process these multi-byte character sets without hanging. (BZ#479151)
- certain output control option combinations could cause the grep tool to segmentation fault. With this updated package, these combinations work as expected and no longer cause a segmentation fault. (BZ#452127)

- the example attached to the "--label" option description was not illustrative enough: as documented, the option actually had no effect. The updated package contains an improved example that shows the "--label" option's utility, both in the manual and info pages. (BZ#484366)

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

1.75. grub

1.75.1. RHBA-2009:1388: bug fix and enhancement update

An updated grub package that fixes a bug and adds an enhancement is now available.

The GRUB utility is responsible for booting the operating system kernel.

This update addresses the following bug:

- current GCC defaults mean grub is compiled without writable string support. On systems with an XFS file system present on the same controller as the boot disk, this could cause the grub shell to segfault and crash. With this update grub no longer assumes constant strings in the XFS file system driver are writable, obviating the error. (BZ#496949)

And adds the following enhancement:

- previously, grub-install did not support installing on virtio_blk devices. When attempted it printed the error message "[device path] does not have any corresponding BIOS drive." With this update, support has been added for installing to virtio devices. (BZ#498388)

All grup users are advised to install this updated package, which resolves this issue and adds this enhancement.

1.76. gstreamer-plugins-base

1.76.1. RHSA-2009:0352: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0352

Updated gstreamer-plugins-base packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GStreamer is a streaming media framework based on graphs of filters which operate on media data. GStreamer Base Plug-ins is a collection of well-maintained base plug-ins.

An integer overflow flaw which caused a heap-based buffer overflow was discovered in the Vorbis comment tags reader. An attacker could create a carefully-crafted Vorbis file that would cause an application using GStreamer to crash or, potentially, execute arbitrary code if opened by a victim. (CVE-2009-0586)

All users of gstreamer-plugins-base are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, all applications using GStreamer (such as Totem or Rhythmbox) must be restarted for the changes to take effect.

1.77. gstreamer-plugins-good

1.77.1. RHSA-2009:1123: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1123

Updated gstreamer-plugins-good packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GStreamer is a streaming media framework, based on graphs of filters which operate on media data. GStreamer Good Plug-ins is a collection of well-supported, good quality GStreamer plug-ins.

Multiple integer overflow flaws, that could lead to a buffer overflow, were found in the GStreamer Good Plug-ins PNG decoding handler. An attacker could create a specially-crafted PNG file that would cause an application using the GStreamer Good Plug-ins library to crash or, potentially, execute arbitrary code as the user running the application when parsed. (CVE-2009-1932)

All users of gstreamer-plugins-good are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. After installing the update, all applications using GStreamer Good Plug-ins (such as some media playing applications) must be restarted for the changes to take effect.

1.77.2. RHSA-2009:0271: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0271

Updated gstreamer-plugins-good packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

GStreamer is a streaming media framework, based on graphs of filters which operate on media data. GStreamer Good Plug-ins is a collection of well-supported, GStreamer plug-ins of good quality released under the LGPL license.

Multiple heap buffer overflows and an array indexing error were found in the GStreamer's QuickTime media file format decoding plugin. An attacker could create a carefully-crafted QuickTime media .mov file that would cause an application using GStreamer to crash or, potentially, execute arbitrary code if played by a victim. (CVE-2009-0386, CVE-2009-0387, CVE-2009-0397)

All users of gstreamer-plugins-good are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the update, all applications using GStreamer (such as totem or rhythmbox) must be restarted for the changes to take effect.

1.78. gtk-vnc

1.78.1. RHBA-2009:1301: bug fix update

An updated gtk-vnc package that fixes several bugs is now available.

gtk-vnc is a VNC viewer widget for GTK. It is built using co-routines allowing it to be completely asynchronous while remaining single threaded.

This update addresses the following issues:

- the handling of the virtual mouse pointer could result in the pointer getting stuck against an invisible wall, unable to move into some areas of the virtual machine display area. (BZ#487560)
- handling of non-US layout keyboards had flaws making it impossible to type certain key sequences, for example Shift+Tab. (BZ#357491)
- the gtk-vnc package was re-based to version 0.3.8, from version 0.3.2, to address problems with virtual mouse pointer movement handling and the conversion of "keysyms" for non-US layout keyboards. The update also improves interoperability with VNC servers and extensions. (BZ#489326)

All gtk-vnc users should install this updated package which addresses these issues.

1.79. hal

1.79.1. RHBA-2009:1359: bug fix and enhancement update

An updated hal package that fixes various bugs and adds several enhancements is now available.

HAL is daemon for collection and maintaining information from several sources about the hardware on the system. It provides a live device list through D-BUS.

Bugs fixed in these updated packages include:

- hal now detects blank optical media correctly on buggy hardware. (BZ#488265)
- if a device identifier was not well formed, the error message the presented was not correctly formatted. This has been fixed. (BZ#471004)
- if an error occurrs the correct hal-device code is now returned. (BZ#462453)
- permissions on the directory /usr/lib/hal were incorrect. hal now owns this directory, as expected. (BZ#481806)
- hal no longer tries to close shared DBus connections to avoid printing a warning. (BZ#472199)
- the hal daemon now starts earlier in the boot sequence, allowing other services to use HAL. (BZ#500577)
- another ID match was added to fix suspending on Lenovo X61s type 7667 notebooks. (BZ#456277)
- the number of brightness levels is now reported correctly for newer laptops using the ibm-acpi driver. (BZ#475850)
- storage devices on the cciss bus are now detected. (BZ#489982)

As well, this update includes the following enhancements:

- new man pages for the installed binaries. (BZ#217644)
- the child-timeout can now be set for machines with a large number of devices. (BZ#463128)

1.80. htdig

1.80.1. RHBA-2009:0291: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0291

Updated htdig packages that resolve several issues are now available.

The ht://Dig system is a complete World Wide Web indexing and searching system for a small domain or intranet. This system is not meant to replace the need for powerful Internet-wide search systems like Lycos, Infoseek, Webcrawler and AltaVista. Instead, it is intended to cover the search needs for a single company, campus, or even a particular subsection of a website. As opposed to some WAIS-based or web server-based search engines, ht://Dig can span several web servers at a site, as long as they understand the HTTP 1.0 protocol.

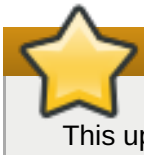
These updated htdig packages provide fixes for the following bugs:

- updating the htdig packages incorrectly removed configuration files, which were written over with the original configuration files. This no longer occurs with these updated packages.
- in cases where htdig attempted to run the parser configured in the "external_parsers" attribute in the htdig.conf configuration file, and running that parser failed, then htdig could attempt to parse its own error messages. With this update, htdig is prevented from parsing data incorrectly in such a manner, exits from such a situation correctly, and displays an improved error message when running the external parser fails.
- running "htfuzzy soundex" after indexing with htdig resulted in spurious error messages when the "allow_numbers" attribute of the htdig.conf configuration file was set to set to true.
- calling either the "htstat" or "htfuzzy" command when the database contained zero words resulted in a segmentation fault, which has been fixed in these updated packages.

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

1.81. httpd

1.81.1. RHSA-2009:1148: Important security update



Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1148

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

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Apache HTTP Server is a popular Web server.

A denial of service flaw was found in the Apache mod_proxy module when it was used as a reverse proxy. A remote attacker could use this flaw to force a proxy process to consume large amounts of CPU time. (CVE-2009-1890)

A denial of service flaw was found in the Apache mod_deflate module. This module continued to compress large files until compression was complete, even if the network connection that requested the content was closed before compression completed. This would cause mod_deflate to consume large amounts of CPU if mod_deflate was enabled for a large file. (CVE-2009-1891)

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.

1.81.2. RHSA-2009:1075: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1075

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

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Apache HTTP Server is a popular and freely-available Web server.

A flaw was found in the handling of compression structures between mod_ssl and OpenSSL. If too many connections were opened in a short period of time, all system memory and swap space would be consumed by httpd, negatively impacting other processes, or causing a system crash. (CVE-2008-1678)

Note: The CVE-2008-1678 issue did not affect Red Hat Enterprise Linux 5 prior to 5.3. The problem was introduced via the RHBA-2009:0181 errata in Red Hat Enterprise Linux 5.3, which upgraded OpenSSL to the newer 0.9.8e version.

A flaw was found in the handling of the "Options" and "AllowOverride" directives. In configurations using the "AllowOverride" directive with certain "Options=" arguments, local users were not restricted from executing commands from a Server-Side-Include script as intended. (CVE-2009-1195)

All httpd users should upgrade to these updated packages, which contain backported patches to resolve these issues. Users must restart httpd for this update to take effect.

1.81.3. RHBA-2009:1380: bug fix update

Updated httpd packages that fix various bugs are now available.

The Apache HTTP Server is a popular and freely-available Web server.

These updated httpd packages provide fixes for the following bugs:

- Apache's mod_mime_magic module attempts to determine the MIME type of files using heuristic tests. However, the "magic" file used by the mod_mime_magic module was unable to detect PNG images correctly as being of MIME type "image/png", which this update corrects. (BZ#240844)

- when using a reverse-proxy configuration with the mod_nss module being used in place of the usual mod_ssl module, the mod_proxy module failed to pass the hostname, which resulted in this error message: "Requested domain name does not match the server's certificate". The hostname is now passed correctly so that secure HTTP (https) connections no longer fail due to this error. (BZ#479410)
- the "mod_ssl" module placed a hard-coded 128K limit on the amount of request body data which would be buffered if an SSL renegotiation was required in a Location or Directory context. This could occur if a POST request was made to a Directory or Location which required client certificate authentication. The limit on the amount of data to buffer is now configurable using the "SSLRenegBufferSize" directive. (BZ#479806)
- when configuring a reverse proxy using an .htaccess file (instead of httpd.conf) by using a "RewriteRule" to proxy requests using the "[P]" flag, space characters in URIs would not be correctly escaped in remote server requests, resulting in "404 Not Found" response codes. This has been fixed so that .htaccess-configured reverse proxies perform proper character-escaping. (BZ#480604)
- if an error occurred when invoking a CGI script, the "500 Internal Server Error" error document was not generated. (BZ#480932)
- the mod_speling module attempts to correct misspellings of URLs. When the "AcceptPathInfo" directive was not enabled, then mod_speling did not handle and correct misspelled directory names. This has been fixed so that directory names are always handled, and possibly corrected, by the mod_speling module, regardless of the value that "AcceptPathInfo" is set to. (BZ#485524)
- if request body data was buffered when an SSL renegotiation was required in a Location or Directory context, then the buffered data was discarded if an internal redirect occurred. (BZ#488886)
- the httpd init script did not reference the process ID stored by a running daemon, and invocations could affect other httpd processes running on the system. (BZ#491135)
- during a graceful restart, a spurious "Bad file descriptor" error message was sometimes logged. The error, though harmless, occurred because the socket on which the server called the accept() function was immediately closed in child processes upon receipt of the graceful restart signal. This error message is no longer logged. (BZ#233955)
- during a graceful restart, the following spurious error messages were logged by the mod_rewrite module if the "RewriteLog" directive was configured: "apr_global_mutex_lock(rewrite_log_lock) failed". (BZ#493023)
- Apache's mod_ext_filter module sometimes logged this spurious error message if an input filter was configured and an error response was sent: "Bad file descriptor: apr_file_close(child input)". (BZ#479463)
- the "%p" format option in the "CustomLog" directive, used to log a port number in a request, did not respect the "remote" and "local" specifiers. (BZ#493070)
- the httpd package inappropriately obsoleted the "mod_jk" package; it no longer does so. (BZ#493592)
- an invalid HTTP status code—such as 70007—was logged to the access log if a timeout or other input error occurred while reading the request body during processing of a CGI script. (BZ#498170)
- a security issue fix (CVE-2009-1195) in Server-Side Include (SSI) Options-handling inadvertently broke backwards-compatibility with the mod_perl module. (BZ#502998)

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

1.82. hwbrowser

1.82.1. RHBA-2009:0277: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0277

An updated hwbrowser package that fixes a bug is now available.

Hwbrowser is a browser for the current hardware configuration.

This updated package contains the following bug fix:

- both hal-device-manager and hwbrowser used the same name ("Hardware") in the System>Administration menu, as well as the same icon (hwbrowser.png). The existence of two apparently identical entries in the menu that launch two different applications could be confusing to users. Since hwbrowser is now a legacy tool, it no longer creates a menu item upon installation, thus eliminating the potential confusion. Users can still run hwbrowser from the command line.

Users should upgrade to this updated package, which resolves this issue.

1.83. hwdata

1.83.1. RHEA-2009:1348: enhancement update

An updated hwdata package that adds enhancements is now available.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

This updated package includes the following additional entries to the Red Hat Enterprise Linux 5.4 pci.ids and usb.ids databases:

- LSI Fusion-MPT SAS-2 controllers (BZ#475674)
- ASPEED Technology AST2000 updated to reflect product name revision in hal-device-manager. AST2000 should now display ASPEED Graphics Family. (BZ#480560)
- Emulex OneConnect 10Gb NIC, Emulex OneConnect 10Gb FCoE Initiator and Emulex OneConnect 10Gb iSCSI Initiator (BZ#496877 , BZ#502907)
- Mellanox Technologies ConnectX EN 10GigE (BZ#501955)
- Intel IGB Virtual Function devices (BZ#502873)
- QLogic Corp. 10GbE Converged Network Adapters (BZ#504035)

Users of hwdata are advised to upgrade to this updated package, which adds these enhancements.

1.84. ia32el

1.84.1. RHBA-2009:1271: bug fix and enhancement update

An ia32el update that features a new release of ia32el, adds support for SSE4.2 instructions, and fixes several bugs is now available.

The ia32el package contains the IA-32 Execution Layer platform, which allows emulation of IA-32 binaries on

Intel Itanium processors.

This updated package fixes the following bugs:

- if SELinux is in Enforcing mode, the 'allow_unconfined_execmem_dyntrans', 'allow_execmem' and 'allow_execstack' booleans must be enabled in order for the IA-32 Execution Layer (i.e. the ia32el service) to operate correctly. If only the 'allow_execmem' or 'allow_execstack' booleans are enabled, the ia32el service can still support emulation; however, SELinux might issue an AVC denial to the service. In previous releases, whenever SELinux issued an AVC denial to ia32el, users were not informed that these booleans needed to be enabled first. This release provides proper documentation (in the README file) for this requirement, and revises the init script to warn the user if any of these boolean requirements are not met at runtime. (BZ#474152)

- this update also fixes a bug that caused the fcntl system call to fail whenever the 'flock' structure was filled with values exceeding 2GB. (BZ#494004)

With this update, the IA-32 Execution Layer is now at version V7:

- this adds support for the latest system calls and SSE4.2 instructions. In addition, this update also applies several fixes from upstream to improve performance, compatibility, and robustness. (BZ#472843)

Users of the IA-32 Execution Layer should upgrade to this update.

1.85. icu

1.85.1. RHSA-2009:1122: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1122

Updated icu packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The International Components for Unicode (ICU) library provides robust and full-featured Unicode services.

A flaw was found in the way ICU processed certain, invalid byte sequences during Unicode conversion. If an application used ICU to decode malformed, multibyte character data, it may have been possible to bypass certain content protection mechanisms, or display information in a manner misleading to the user. (CVE-2009-0153)

All users of icu should upgrade to these updated packages, which contain backported patches to resolve this issue.

1.85.2. RHSA-2009:0296: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0296

Updated icu packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The International Components for Unicode (ICU) library provides robust and full-featured Unicode services.

A flaw was found in the way ICU processed certain, invalid, encoded data. If an application used ICU to decode malformed, multibyte, character data, it may have been possible to bypass certain content protection mechanisms, or display information in a manner misleading to the user. (CVE-2008-1036)

All users of icu should upgrade to these updated packages, which contain backported patches to resolve these issues.

1.86. initscripts

1.86.1. RHBA-2009:1344: bug fix update

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

- previously, when using the disk encryption feature to encrypt the root filesystem, the following error message was returned on the console when shutting down the system:

  ```
  Stopping disk encryption [FAILED]
  ```

  with this update, this message is no longer displayed.(BZ#471944)

- previously, if a vlan device was a member of a bridge, and the vlan device was removed from the bridge the vlan interface was not removed. With this update, the ifdown script has been updated to remove vlan interfaces if the device is removed from the bridge. (BZ#481557, BZ#463325)

- in some cases, when network service failed to restart, the /etc/init.d/network initscript would return an incorrect status of "0". With this update, /etc/init.d/network has been modified to return 1 if the service fails to start or if any NIC fails to get an address. (BZ#481002)

- a bonding device cannot be added to a bridge until at least one slaved ethernet interface has been added to the bridge. Previously, the order of commands in ifup-eth script attempted to add a bonding device prior to the ethernet interface being added. With this update, this issue has been resolved. (BZ#463014)

- previously, if a suspend or hibernate action did not complete, the "/.suspended" file may have persisted thorough a reboot. Consequently, if the system is rebooted, and another suspend or hibernate action is invoked, the system would fall back to a virtual terminal display. With this update, the rc.sysinit script now removes the "/.suspended" file during the boot sequence, which resolves this issue. (BZ#270861)

- previously, the ifup-ipsec initscript did not allow the Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols to be initialized independently. With this update, configuration parameters are now implemented in ifup-ipsec, allowing these protocols to be activated seperately. (BZ#251494)

- previously, support for raw devices in the upstream kernel was deprecated. However, this support has been returned to the kernel. Consequently, in Red Hat Enterprise Linux 5.4, support for raw devices has also been returned. In this update, the initscripts packages have been updated, allowing rawdevices to again be configured by editing /etc/sysconfig/rawdevices. (BZ#472891)

- previously, the rc.sysinit script incorrectly handled the clean-up of sub-directories in "/var/run/libvirt/". Consequently, rc.sysinit could not remove the "/var/run/libvirt/network/" and "/var/run/libvirt/qemu/" directories. With this update rc.sysinit now correctly removes these directories. (BZ#505600)

- previously, the /etc/init.d/network script initialized ipsec tunnels before vlan interfaces. Consequently, route handling traffic was not created between tunneled networks as the tunneled network was not yet configured. With this update, this issue has been resolved. (BZ#481733)
- The documentation for the /etc/sysconfig/ directory (located at /usr/share/doc/initscript-<version>/sysconfig.txt) has been updated with information about BONDING_OPS. (BZ#472480)
- previously, ctc and netiucv devices may not have been initialized automatically during boot. With this update, the ifup-ctc and ifup-iucv initscripts have been changed to resolve this issue.(BZ#475721)
- systems that have both an NFS server and a client with NFS shares mounted, running the "service netfs stop" command will correctly unmount the NFS shares. Previously, however, this command also unmounted "/proc/fs/nfsd", which is required by the NFS server. Consequently, after running this command to unmount NFS shares, clients would be unable to mount shares on the NFS server based on that machine. With this update, the netfs initscript has been updated, resolving this issue. (BZ#481794)
- previously netfs initialized multiple device (MD) arrays (using the mdadm command) before LVM was initialized. Consequently, an MD array of iSCSI devices would not initialize automatically. With this update, the netfs script has been updated, resolving this issue. (BZ#480627)
- previously, if a GFS2 filesystem is listed in /etc/fstab, rc.sysinit would fail when attempting to mount the filesystem, as the cluster services had not been not started yet. With this update, the initscripts have been updated to resolve this issue. (BZ#494963)
- the ifup initscript has been updated to ensure HiperSocket VLAN support is initialized correctly during boot. (BZ#490584)
- previously, adding networking routes using the system-config-network-gui resulted in the following error message being displayed:

  ```
  /lib/udev/ccw_init: line 31: echo: write error: Operation not permitted
  ```

  With this update the initscripts have been fixed, allowing the use of system-config-networking-gui to add network routes. (BZ#484411)

Users are advised to upgrade to this updated package, which resolves these issues.

1.87. iptables

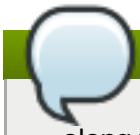
1.87.1. RHBA-2009:1414: bug fix and enhancement update

Updated iptables packages that fix several bugs and add an enhancement are now available.

The iptables utility controls the network packet filtering code in the Linux kernel.

These updated iptables packages provide the following enhancement:

- while its IPv4 counterpart was present, the Differentiated Services Code Point (DSCP) match target for IPv6 was missing. Two new modules, one for iptables and a separate one for the Linux kernel, now enable this functionality.



Note

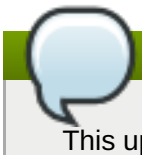
along with this iptables update, the kernel update for Red Hat Enterprise Linux 5.4 must be installed, and the system must be rebooted, in order to enable Differentiated Services Code Point (DSCP) match target functionality for IPv6. (BZ#480371)

In addition, these updated iptables packages provide fixes for the following bugs:

- the init scripts for iptables and ip6tables sometimes exited with incorrect or invalid exit statuses. (BZ#242457)
- the Internet Control Message Protocol (ICMP) '--reject-with' types did not always work as expected. This has been fixed in these updated packages. (BZ#253014)
- the iptables-restore(8) man page did not contain descriptions of some of the options that were listed in the program's help information. These information sources for the utility's options have now been synchronized. (BZ#474847)
- the "ROUTE" section of the iptables(8) man page contained misleading information on certain features that do not exist in the iptables packages. (BZ#485834)
- the iptables-devel package did not include certain header files, which are now included in the updated package. (BZ#487649)
- the spec file contained a typo on the the Release line. (BZ#440622)

1.88. iproute

1.88.1. RHBA-2009:0404: bug fix update



Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0404

An updated iproute package that fixes a bug is now available.

The iproute package contains networking utilities such as ip and rtmon, which use the advanced networking capabilities of the Linux 2.4 and 2.6 kernels.

This updated iproute package fixes a bug which resulted in stack corruption when the command "ip maddr show" was used with an InfiniBand address. This occurred because the length of an InfiniBand address did not fit into the 16-byte field in which it was stored. With this update, the InfiniBand address is stored correctly, thus preventing possible stack corruption.

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

1.89. iprutils

1.89.1. RHBA-2009:1246: bug fix and enhancement update

An iprutils update that fixes a buffer alignment bug and improves the performance of supported SSDs is now available.

The iprutils package provides a suite of utilities to manage and configure SCSI devices supported by the ipr SCSI storage device driver.

This update addresses the following bug and adds the following enhancement:

- a buffer alignment problem prevented iprconfig from updating disk microcode during I/O. In the block layer, iprconfig incorrectly used malloc() for memory allocation; as a result, buffers in the scatter/gather list were not 512-byte aligned. With this update, iprconfig uses posix_memalign() to properly execute memory allocation, which corrects the buffer alignment problem. This update also applies several other improvements to help ensure that iprconfig can perform disk microcode updates even during heavy I/O. (BZ#452312)
- this update also applies a firmware enhancement to support dual-shared Active/Active multiplex on SAS adapters. This improves the performance of supported solid-state disks (SSD). (BZ#475362)

Users of iprutils and the ipr driver are advised to apply this update.

1.90. ipsec-tools

1.90.1. RHSA-2009:1036: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1036

An updated ipsec-tools package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The ipsec-tools package is used in conjunction with the IPsec functionality in the Linux kernel and includes racoon, an IKEv1 keying daemon.

A denial of service flaw was found in the ipsec-tools racoon daemon. An unauthenticated, remote attacker could trigger a NULL pointer dereference that could cause the racoon daemon to crash. (CVE-2009-1574)

Multiple memory leak flaws were found in the ipsec-tools racoon daemon. If a remote attacker is able to make multiple connection attempts to the racoon daemon, it was possible to cause the racoon daemon to consume all available memory. (CVE-2009-1632)

Users of ipsec-tools should upgrade to this updated package, which contains backported patches to correct these issues. Users must restart the racoon daemon for this update to take effect.

1.91. iputils

1.91.1. RHBA-2009:1090: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1090

An updated iputils package that fixes a bug is now available.

The iputils package contains basic utilities for monitoring a network, including ping.

This updated iputils package fixes the following bug:

- it is the rdisc utility which is called at boot time to populate the network routing tables with default routes. This bug caused rdisc to fail during initialization when more than one IP address was assigned to a single interface. This has been solved so that when rdisc encounters two or more IP addresses assigned to the same interface, it continues working as expected. (BZ#470498)

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

1.92. ipvsadm

1.92.1. RHBA-2009:1398: bug fix update

Updated ipvsadm packages that fix several bugs are now available.

ipvsadm is a utility to administer the IP Virtual Server services offered by the Linux kernel.

This update fixes the following bugs:

- running "service ipvsadm status" returned the status code "0" (for "service is running") even when ipvsadm was stopped. The ipvsadm init script has been updated and ipvsadm now only returns "0" when it is, in fact, running. (BZ#232335)
- ipvsadm's previous start priority, 08, meant it loaded before network. If the ipvsadm rule set contained virtual services using fwmarks, these rules did not load properly. ipvsadm's start priority is now 11, ensuring it loads after network and ensuring virtual services load after real network services. (BZ#472425)
- previously you could install the debuginfo packages but, because the makefile stripped the symbol table, they contained no data. The ipvsadm makefile no longer strips the symbol table and installing the debuginfo packages adds ipvsadm.debug and the debugging source as expected. (BZ#500601)

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

1.93. irqbalance

1.93.1. RHBA-2009:1265: bug fix update

An updated irqbalance package that fixes various bugs is now available.

irqbalance is a daemon that evenly distributes IRQ load across multiple CPUs for enhanced performance.

This updated package addresses several minor bugs:

- multiple instances of irqbalance could be started when changing between run levels. A universal exit is now run on existing instances so that only one will operate at a time. (BZ#471574)

- several errors in set_interrupt_count and investigate interaction caused irqbalance to ignore IRQBALANCE_BANNED_INTERRUPTS. The two now work discretely and the problem no longer presents. (BZ#479459)
- documentation has been improved in order to clarify the meaning and use of some of the configuration settings in irqbalance. (BZ#479856)

Users are advised to upgrade to this updated irqbalance package, which resolves these issues.

1.94. iscsi-initiator-utils

1.94.1. RHBA-2009:1099: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1099

An updated iscsi-initiator-utils package that fixes a bug is now available.

The iscsi-initiator-utils package provides the server daemon for the 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.

This updated iscsi-initiator-utils package fixes the following bug:

- attempting to log in to targets which used the iSCSI protocol's login redirect feature failed due to a coding error in the IPv6 address parser. This bug has been fixed in this updated package so that address parsing succeeds as expected, and logging in to targets over IPv6 is once again possible. (BZ#501737)

All users using IPv6 with LUN targets which employ login redirect, such as EqualLogic targets, should upgrade to this updated package, which resolves this issue.

1.94.2. RHBA-2009:1368: bug fix update

An updated iscsi-initiator-utils package that fixes various bugs and adds support for Chelsio and Broadcom iSCSI cards is now available

The iscsi package provides the server daemon for the 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.

Bugs fixed and enhancements added in this updated package include:

- iscsi-initiator-utils now includes support for Broadcom bnx2 and bnx2x network interface cards. (BZ#442418)
- iscsi-initiator-utils has been rebased to upstream version 2.0-870. Among many other changes, this version supports the offload feature of Broadcom and Chelsio cards. Refer to the changelog included in the package for a full list of bug fixes and enhancements in this version. Section 5.1.2 of /usr/share/docs/iscsi-initiator-utils-$version/README contains instructions to set up ifaces for use with offload cards. (BZ#458203)

- the iscsi-initiator-utils packages place files in the /etc/iscsi directory but previously, did not list that directory for creation. The /etc/iscsi directory would therefore be created during the installation process, but would remain unowned. /etc/iscsi is now listed for creation and are therefore owned by iscsi-initiator-utils. (BZ#481807)

- when a user-space iSCSI tool invokes an option that is not supported in the kernel, the tool returns "Iferror -38". Previously, this error message was presented to users and could mislead them to think that a problem existed with their iSCSI configuration. The iSCSI tools no longer present this type of error to users and therefore do not create this potential misunderstanding. Note that certain combinations of new tools with old kernels might still present a related "-22" error. (BZ#497940)

- the iSCSI protocol allows targets to redirect initiators during the login phase. Previously, the code used by the iscsi initiator to parse IPv6 addresses contained faulty logic that caused it to fail to recognize IPv6 addresses as valid when redirected. As a consequence, when operating in an IPv6 environment, the initiator could not log into targets that use the login redirect feature, such as Dell EqualLogic targets. The initiator now parses IPv6 addresses correctly, enabling use of these targets in IPv6 environments. (BZ#500102)

- previously, the cxgb3i driver for Chelsio host bus adapters (HBAs) was not listed in the iscsi init script. Therefore, iscsi would not load this driver and therefore could not use the Chelsio HBAs that need this driver. The cxgb3i driver is now included in the iscsi init script, which enables the use of these devices. (BZ#505958)

- the iscsi code contained a bad cast of a data structure. This would lead to a segmentation fault while logging in or out of an iSCSI target. With the logic now corrected, these segmentation faults do not occur. (BZ#508782)

- iscsiadm obtains its information about the boot environment from the iSCSI boot firmware table (IBFT). However, this information does not include the target portal group tag (TPGT) associated with the boot target. Iscsiadm would assume that the relevant TPGT should be "1". In cases where this was correct, the boot process would continue as intended. In all other cases, iscsiadm would be unable to find the target necessary for the boot to proceed. This made it impossible to automate the installation of Red Hat Enterprise Linux in environments with multiple portals on targets and where the portal used for boot did not have TPGT=1. Iscsiadm no longer assumes a value for the TPGT for the boot portal and instead relies on the information that it finds in the /var/lib/iscsi record. This enables iscsiadm to find the correct target automatically, and therefore makes automated installations possible. (BZ#515806)

Users should upgrade to this updated package, which resolves these issues.

1.95. isdn4k-utils

1.95.1. RHBA-2009:1112: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1112

Updated isdn4k-utils packages that resolve several issues are now available.

The isdn4k-utils packages contain a collection of utilities needed for configuring an ISDN subsystem.

These updated isdn4k-utils packages provide fixes for the following bugs:

- the init scripts for the "capi" and "isdn" programs sometimes exited with incorrect or invalid exit statuses.

These init scripts have been updated for compliance with Linux Standard Base (LSB) guidelines. The "capi" and "isdn" programs now exit with exit status 5 (program is not installed) or 6 (program is not configured), as appropriate. The improved init scripts also check for correct privileges and exit with exit status 4 (user has insufficient privileges) when appropriate. (BZ#237831)

- the isdn4k-utils packages contained spurious CVS files; they have been removed in these updated packages. (BZ#481569)
- the divaload, divalog, divalogd and ipppd executable binaries, which were located in the /sbin directory, depend on libraries located in the /usr/lib directory. In certain situations such as when located on a separate partition, the /usr directory may not be mounted and available when the executables are called. For this reason, divaload, divalog, divalogd and ipppd have all been moved to the /usr/sbin directory, which solves this potential problem. (BZ#503910)

All users of isdn4k-utils are advised to upgrade to these updated packages, which resolve these issues.

1.96. iwl3945-firmware

1.96.1. RHEA-2009:1253: enhancement update

An enhanced iwl3945-firmware package is now available.

The iwl3945-firmware package provides the iwl3945 wireless driver with the firmware it requires in order to function correctly with iwl3945 hardware.

This updated iwl3945-firmware package adds the following enhancement:

- The iwl3945 driver and the iwl3945 firmware work together to provide proper wireless functionality. It is best to pair equivalent versions of these components in order to provide maximum compatibility between them, which this updated package provides.

Users of wireless devices using the iwl3945 driver are advised to upgrade to this updated package, which adds this enhancement.

1.97. iwl4965-firmware

1.97.1. RHEA-2009:1252: enhancement update

An enhanced iwl4965-firmware package is now available.

The iwl4965-firmware package provides the iwlagn wireless driver with the firmware it requires in order to function correctly with iwlagn hardware.

This updated iwl4965-firmware package adds the following enhancement:

- the iwlagn driver and the iwl4965 firmware work together to provide proper wireless functionality. It is best to pair equivalent versions of these components in order to provide maximum compatibility between them, which this updated package provides. (BZ#476869)

Users of wireless devices which use iwl4965 firmware are advised to upgrade to this updated package, which adds this enhancement.

1.98. jadetex

1.98.1. RHBA-2009:0378: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0378

An updated jadetex package that fixes several bugs is now available.

The jadetex package contains high-level TeX macros which can be used to produce DVI, PostScript and/or Portable Document Format (PDF) output.

This updated jadetex package includes fixes for the following bugs:

- several jadetex files which were installed in the /usr/share/texmf/web2c/ directory had the wrong SELinux context. This updated package corrects the SELinux context of these files.
- previously, installing the jadetex package led to the creation of two unnecessary log files that were not owned by the package in the /usr/share/texmf/web2c/ directory. This updated package no longer creates these log files, thus resolving the issue.

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

1.99. java-1.4.2-ibm

1.99.1. RHSA-2009:0445: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0445

Updated java-1.4.2-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 3 Extras, Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The IBM® 1.4.2 SR13 Java™ release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. These vulnerabilities are summarized on the IBM "Security alerts" page listed in the References section. (CVE-2008-2086, CVE-2008-5339, CVE-2008-5340, CVE-2008-5342, CVE-2008-5343, CVE-2008-5344, CVE-2008-5345, CVE-2008-5346, CVE-2008-5348, CVE-2008-5350, CVE-2008-5351, CVE-2008-5353, CVE-2008-5354, CVE-2008-5359, CVE-2008-5360)

All users of java-1.4.2-ibm are advised to upgrade to these updated packages, which contain the IBM 1.4.2 SR13 Java release. All running instances of IBM Java must be restarted for the update to take effect.

1.100. java-1.5.0-ibm

1.100.1. RHEA-2009:1208: enhancement update

Note

This update has already been released (prior to the GA of this release) as errata RHEA-2009:1208

Updated java-1.5.0-ibm packages that comprise IBM's Java 1.5.0 SR10 release are now available.

The following packages comprise IBM's 1.5.0 SR10 Java release:

java-1.5.0-ibm java-1.5.0-ibm-demo java-1.5.0-ibm-devel java-1.5.0-ibm-javacomm java-1.5.0-ibm-jdbc java-1.5.0-ibm-plugin java-1.5.0-ibm-src

These packages include the IBM Java 5 Runtime Environment and the IBM Java 5 Software Development Kit.

The Java 5 Runtime Environment (JRE) consists of the Java virtual machine, the Java platform core classes and supporting files, and includes a Web browser plug-in for running Java applets. It is the runtime section of the Java 5 SDK, but without the development tools such as compilers and debuggers.

The Java 5 Software Development Kit (SDK) is a development environment for building applications, applets, and components that can be deployed on the Java platform. The Java 5 SDK software includes tools useful for developing and testing programs written in the Java programming language. The Java 5 SDK software also includes a JDBC/ODBC bridge for Java applications that need to communicate with a database.

These updated packages comprise the IBM Java 5 SR10 release.

Users of java-1.4.2-ibm may install these new 1.5.0 packages in parallel and switch between the new and old Java environments using the alternatives tool.

1.100.2. RHSA-2009:1038: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1038

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras and 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. These vulnerabilities are summarized on the IBM "Security alerts" page listed in the References section. (CVE-2009-1093, CVE-2009-1094, CVE-2009-1095, CVE-2009-1096, CVE-2009-1097, CVE-2009-1098, CVE-2009-1099, CVE-2009-1100, CVE-2009-1101, CVE-2009-1103, CVE-2009-1104, CVE-2009-1105, CVE-2009-1106, CVE-2009-1107)

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.5.0 SR9-SSU Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.101. java-1.5.0-sun

1.101.1. RHSA-2009:1199: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1199

Updated java-1.5.0-sun packages that correct several security issues are now available for Red Hat Enterprise Linux 4 Extras and 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The Sun 1.5.0 Java release includes the Sun Java 5 Runtime Environment and the Sun Java 5 Software Development Kit.

This update fixes several vulnerabilities in the Sun Java 5 Runtime Environment and the Sun Java 5 Software Development Kit. These vulnerabilities are summarized on the "Advance notification of Security Updates for Java SE" page from Sun Microsystems, listed in the References section. (CVE-2009-2475, CVE-2009-2625, CVE-2009-2670, CVE-2009-2671, CVE-2009-2672, CVE-2009-2673, CVE-2009-2675, CVE-2009-2676, CVE-2009-2689)

Users of java-1.5.0-sun should upgrade to these updated packages, which correct these issues. All running instances of Sun Java must be restarted for the update to take effect.

1.101.2. RHSA-2009:0394: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0394

Updated java-1.5.0-sun packages that correct several security issues are now available for Red Hat Enterprise Linux 4 Extras and 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The Sun 1.5.0 Java release includes the Sun Java 5 Runtime Environment and the Sun Java 5 Software Development Kit.

This update fixes several vulnerabilities in the Sun Java 5 Runtime Environment and the Sun Java 5 Software Development Kit. These vulnerabilities are summarized on the "Advance notification of Security Updates for Java SE" page from Sun Microsystems, listed in the References section. (CVE-2006-2426, CVE-2009-1093, CVE-2009-1094, CVE-2009-1095, CVE-2009-1096, CVE-2009-1098, CVE-2009-1099, CVE-2009-1100, CVE-2009-1103, CVE-2009-1104, CVE-2009-1107)

Users of java-1.5.0-sun should upgrade to these updated packages, which correct these issues. All running instances of Sun Java must be restarted for the update to take effect.

1.102. java-1.6.0-ibm

1.102.1. RHSA-2009:1198: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1198

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras and 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. These vulnerabilities are summarized on the IBM "Security alerts" page listed in the References section. (CVE-2009-1093, CVE-2009-1094, CVE-2009-1095, CVE-2009-1096, CVE-2009-1097, CVE-2009-1098, CVE-2009-1099, CVE-2009-1100, CVE-2009-1101, CVE-2009-1103, CVE-2009-1104, CVE-2009-1105, CVE-2009-1106, CVE-2009-1107)

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR5 Java release. All running instances of IBM Java must be restarted for the update to take effect.

1.102.2. RHSA-2009:0369: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0369

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 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. These vulnerabilities are summarized on the IBM "Security alerts" page listed in the References section. (CVE-2008-5340, CVE-2008-5341, CVE-2008-5342, CVE-2008-5343, CVE-2008-5351, CVE-2008-5356, CVE-2008-5357, CVE-2008-5358)

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR4 Java release. All running instances of IBM Java must be restarted for the update to take effect.

1.103. java-1.6.0-openjdk

1.103.1. RHSA-2009:1201: Important security and bug fix update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1201

Updated java-1.6.0-openjdk packages that fix several security issues and a bug are now available for Red Ha Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit. The Java Runtime Environment (JRE) contains the software and tools that users need to run applications written using the Java programming language.

A flaw was found in the way the XML Digital Signature implementation in the JRE handled HMAC-based XML signatures. An attacker could use this flaw to create a crafted signature that could allow them to bypass authentication, or trick a user, applet, or application into accepting untrusted content. (CVE-2009-0217)

Several potential information leaks were found in various mutable static variables. These could be exploited in application scenarios that execute untrusted scripting code. (CVE-2009-2475)

It was discovered that OpenType checks can be bypassed. This could allow a rogue application to bypass access restrictions by acquiring references to privileged objects through finalizer resurrection. (CVE-2009-2476)

A denial of service flaw was found in the way the JRE processes XML. A remote attacker could use this flaw to supply crafted XML that would lead to a denial of service. (CVE-2009-2625)

A flaw was found in the JRE audio system. An untrusted applet or application could use this flaw to gain read access to restricted System properties. (CVE-2009-2670)

Two flaws were found in the JRE proxy implementation. An untrusted applet or application could use these flaws to discover the usernames of users running applets and applications, or obtain web browser cookies and use them for session hijacking attacks. (CVE-2009-2671, CVE-2009-2672)

An additional flaw was found in the proxy mechanism implementation. This flaw allowed an untrusted applet or application to bypass access restrictions and communicate using non-authorized socket or URL connections to hosts other than the origin host. (CVE-2009-2673)

An integer overflow flaw was found in the way the JRE processes JPEG images. An untrusted application could use this flaw to extend its privileges, allowing it to read and write local files, as well as to execute local applications with the privileges of the user running the application. (CVE-2009-2674)

An integer overflow flaw was found in the JRE unpack200 functionality. An untrusted applet or application could extend its privileges, allowing it to read and write local files, as well as to execute local applications with the privileges of the user running the applet or application. (CVE-2009-2675)

It was discovered that JDK13Services grants unnecessary privileges to certain object types. This could be misused by an untrusted applet or application to use otherwise restricted functionality. (CVE-2009-2689)

An information disclosure flaw was found in the way private Java variables were handled. An untrusted applet or application could use this flaw to obtain information from variables that would otherwise be private. (CVE-2009-2690)

Note: The flaws concerning applets in this advisory, CVE-2009-2475, CVE-2009-2670, CVE-2009-2671, CVE-2009-2672, CVE-2009-2673, CVE-2009-2675, CVE-2009-2689, and CVE-2009-2690, can only be triggered ir java-1.6.0-openjdk by calling the "appletviewer" application.

This update also fixes the following bug:

- the EVR in the java-1.6.0-openjdk package as shipped with Red Hat Enterprise Linux allowed the java-1.6.0-openjdk package from the EPEL repository to take precedence (appear newer). Users using java-1.6.0-openjdk from EPEL would not have received security updates since October 2008. This update prevents the packages from EPEL from taking precedence. (BZ#499079)

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.

1.103.2. RHSA-2009:0377: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0377

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit. The Java Runtime Environment (JRE) contains the software and tools that users need to run applications written using the Java programming language.

A flaw was found in the way that the Java Virtual Machine (JVM) handled temporary font files. A malicious applet could use this flaw to use large amounts of disk space, causing a denial of service. (CVE-2006-2426)

A memory leak flaw was found in LittleCMS (embedded in OpenJDK). An application using color profiles could use excessive amounts of memory, and possibly crash after using all available memory, if used to open specially-crafted images. (CVE-2009-0581)

Multiple integer overflow flaws which could lead to heap-based buffer overflows, as well as multiple insufficient input validation flaws, were found in the way LittleCMS handled color profiles. An attacker could use these flaws to create a specially-crafted image file which could cause a Java application to crash or, possibly, execute arbitrary code when opened. (CVE-2009-0723, CVE-2009-0733)

A null pointer dereference flaw was found in LittleCMS. An application using color profiles could crash while converting a specially-crafted image file. (CVE-2009-0793)

A flaw in the Java API for XML Web Services (JAX-WS) service endpoint handling could allow a remote attacker to cause a denial of service on the server application hosting the JAX-WS service endpoint. (CVE-2009-1101)

A flaw in the way the Java Runtime Environment initialized LDAP connections could allow a remote, authenticated user to cause a denial of service on the LDAP service. (CVE-2009-1093)

A flaw in the Java Runtime Environment LDAP client could allow malicious data from an LDAP server to cause arbitrary code to be loaded and then run on an LDAP client. (CVE-2009-1094)

Several buffer overflow flaws were found in the Java Runtime Environment unpack200 functionality. An untrusted applet could extend its privileges, allowing it to read and write local files, as well as to execute local applications with the privileges of the user running the applet. (CVE-2009-1095, CVE-2009-1096)

A flaw in the Java Runtime Environment Virtual Machine code generation functionality could allow untrusted applets to extend their privileges. An untrusted applet could extend its privileges, allowing it to read and write

local files, as well as execute local applications with the privileges of the user running the applet. (CVE-2009-1102)

A buffer overflow flaw was found in the splash screen processing. A remote attacker could extend privileges to read and write local files, as well as to execute local applications with the privileges of the user running the java process. (CVE-2009-1097)

A buffer overflow flaw was found in how GIF images were processed. A remote attacker could extend privileges to read and write local files, as well as execute local applications with the privileges of the user running the java process. (CVE-2009-1098)

Note: The flaws concerning applets in this advisory, CVE-2009-1095, CVE-2009-1096, and CVE-2009-1102, can only be triggered in java-1.6.0-openjdk by calling the "appletviewer" application.

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.

1.104. java-1.6.0-sun

1.104.1. RHSA-2009:1200: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1200

Updated java-1.6.0-sun packages that correct several security issues are now available for Red Hat Enterprise Linux 4 Extras and 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. These vulnerabilities are summarized on the "Advance notification of Security Updates for Java SE" page from Sun Microsystems, listed in the References section. (CVE-2009-0217, CVE-2009-2475, CVE-2009-2476, CVE-2009-2625, CVE-2009-2670, CVE-2009-2671, CVE-2009-2672, CVE-2009-2673, CVE-2009-2674, CVE-2009-2675, CVE-2009-2676, CVE-2009-2690)

Users of java-1.6.0-sun should upgrade to these updated packages, which correct these issues. All running instances of Sun Java must be restarted for the update to take effect.

1.104.2. RHBA-2009:1093: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1093

Updated java-1.6.0-sun packages are now available for Red Hat Enterprise Linux 5.3 Supplementary.

The java-1.6.0-sun packages include the Sun Java 6 Runtime Environment, Sun Java 6 Software Development Kit (SDK), the source code for the Sun Java class libraries, the Sun Java browser plug-in and Web Start, the Sun JDBC/ODBC bridge driver, and demonstration files for the Sun Java 6 SDK.

These updated java-1.6.0-sun packages upgrade Sun's Java 6 SDK from version 1.6.0_13 to version 1.6.0_14, which provides fixes for a number of bugs. To view the release notes for the bug fixes included in this update, refer to the URL provided in the "References" section of this errata. (BZ#505075)

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which resolve these issues.

1.104.3. RHSA-2009:0392: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0392

Updated java-1.6.0-sun packages that correct several security issues are now available for Red Hat Enterprise Linux 4 Extras and 5 Supplementary.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. These vulnerabilities are summarized on the "Advance notification of Security Updates for Java SE" page from Sun Microsystems, listed in the References section. (CVE-2006-2426, CVE-2009-1093, CVE-2009-1094, CVE-2009-1095, CVE-2009-1096, CVE-2009-1097, CVE-2009-1098, CVE-2009-1099, CVE-2009-1100, CVE-2009-1101, CVE-2009-1102, CVE-2009-1103, CVE-2009-1104, CVE-2009-1105, CVE-2009-1106, CVE-2009-1107)

Users of java-1.6.0-sun should upgrade to these updated packages, which correct these issues. All running instances of Sun Java must be restarted for the update to take effect.

1.104.4. RHEA-2009:0284: enhancement update

Note

This update has already been released (prior to the GA of this release) as errata RHEA-2009:0284

Updated java-1.6.0-sun packages are now available for Red Hat Enterprise Linux 5.3.

The java-1.6.0-sun packages include the Sun Java 6 Runtime Environment, Sun Java 6 Software Development Kit (SDK), the source code for the Sun Java class libraries, the Sun Java browser plug-in and Web Start, the Sun JDBC/ODBC bridge driver, and demonstration files for the Sun Java 6 SDK.

These updated java-1.6.0-sun packages upgrade Sun's Java 6 SDK from version 1.6.0_11 to version 1.6.0_12, which provides fixes for a number of bugs. As well, this update includes a 64-bit Java Plug-In for web browsers. To view the release notes for the bug fixes included in this update, refer to the URL provided in the "References" section of this errata.

Users of java-1.6.0-sun are advised to upgrade to these updated packages, which resolve these issues.

1.105. kdebase

1.105.1. RHBA-2009:1277: bug fix update

Updated kdebase packages that fix various bugs are now available.

The K Desktop Environment (KDE) is a graphical desktop environment for the X Window System. The kdebase packages include core applications for the K Desktop Environment.

These updated packages fix the following bugs:

- version 0.5 of the Hardware Abstraction Layer (HAL) creates child device objects only when a file system is mounted. In cases where a storage device cannot be polled (for example, a floppy drive or IDE Zip drive), HAL adds mount methods to the device itself rather than the volume. Previously, this meant that when used in conjunction with HAL 0.5, KDE 3 would not allow users to mount file systems on devices which the HAL could not poll. KDE now includes a modified HAL back end that allows users to mount and unmount volumes through the storage devices detected by the HAL. (BZ#469723)
- previously, when KDE refreshed desktop icons, it did not refresh the list of icons that it should display on the desktop. As a consequence, icons could appear on the desktop even when the file that they represented had been deleted, and refreshing the desktop would not remove these icons. This situation could arise, for example, when viewing files on an NFS share. When KDE refreshes its view of the desktop, it now updates the list of icons first and therefore avoids drawing icons for non-existent files. (BZ#472295)

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

1.106. kdegraphics

1.106.1. RHSA-2009:1130: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1130

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

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The kdegraphics packages contain applications for the K Desktop Environment (KDE). Scalable Vector Graphics (SVG) is an XML-based language to describe vector images. KSVG is a framework aimed at implementing the latest W3C SVG specifications.

A use-after-free flaw was found in the KDE KSVG animation element implementation. A remote attacker could create a specially-crafted SVG image, which once opened by an unsuspecting user, could cause a denial of service (Konqueror crash) or, potentially, execute arbitrary code with the privileges of the user running Konqueror. (CVE-2009-1709)

A NULL pointer dereference flaw was found in the KDE, KSVG SVGList interface implementation. A remote attacker could create a specially-crafted SVG image, which once opened by an unsuspecting user, would cause memory corruption, leading to a denial of service (Konqueror crash). (CVE-2009-0945)

All users of kdegraphics should upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

1.106.2. RHSA-2009:0431: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0431

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

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kdegraphics packages contain applications for the K Desktop Environment, including KPDF, a viewer for Portable Document Format (PDF) files.

Multiple integer overflow flaws were found in KPDF's JBIG2 decoder. An attacker could create a malicious PDF file that would cause KPDF to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0147, CVE-2009-1179)

Multiple buffer overflow flaws were found in KPDF's JBIG2 decoder. An attacker could create a malicious PDF file that would cause KPDF to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0146, CVE-2009-1182)

Multiple flaws were found in KPDF's JBIG2 decoder that could lead to the freeing of arbitrary memory. An attacker could create a malicious PDF file that would cause KPDF to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0166, CVE-2009-1180)

Multiple input validation flaws were found in KPDF's JBIG2 decoder. An attacker could create a malicious PDF file that would cause KPDF to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0800)

Multiple denial of service flaws were found in KPDF's JBIG2 decoder. An attacker could create a malicious PDF that would cause KPDF to crash when opened. (CVE-2009-0799, CVE-2009-1181, CVE-2009-1183)

Red Hat would like to thank Braden Thomas and Drew Yao of the Apple Product Security team, and Will Dormann of the CERT/CC for responsibly reporting these flaws.

Users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

1.107. kdelibs

1.107.1. RHSA-2009:1127: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1127

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

This update has been rated as having critical security impact by the Red Hat Security Response Team.

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

A flaw was found in the way the KDE CSS parser handled content for the CSS "style" attribute. A remote attacker could create a specially-crafted CSS equipped HTML page, which once visited by an unsuspecting user, could cause a denial of service (Konqueror crash) or, potentially, execute arbitrary code with the privileges of the user running Konqueror. (CVE-2009-1698)

A flaw was found in the way the KDE HTML parser handled content for the HTML "head" element. A remote attacker could create a specially-crafted HTML page, which once visited by an unsuspecting user, could cause a denial of service (Konqueror crash) or, potentially, execute arbitrary code with the privileges of the user running Konqueror. (CVE-2009-1690)

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way the KDE JavaScript garbage collector handled memory allocation requests. A remote attacker could create a specially-crafted HTML page, which once visited by an unsuspecting user, could cause a denial of service (Konqueror crash) or, potentially, execute arbitrary code with the privileges of the user running Konqueror. (CVE-2009-1687)

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

1.108. kdenetwork

1.108.1. RHBA-2009:0452: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0452

Updated kdenetwork packages that resolve an issue are now available.

The kdenetwork packages provide a collection of networking applications for the K Desktop Environment (KDE).

These updated kdenetwork packages fix the following bug:

- the krfb command is a VNC-compatible server for sharing KDE desktops. The desktop can be shared by running krfb from the command line. krfb would fail if a user accessed the shared desktop from a web browser using the address http://hostname:5800 (where hostname is a valid address or hostname). The updated kdenetwork packages no longer have this issue and shared desktops can be accessed normally.

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

1.109. kdepim

1.109.1. RHBA-2009:1057: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1057

Updated kdepim packages that fix a bug are now available.

The K Desktop Environment (KDE) is a graphical desktop for the X Window System. The KDE Personal Information Management (kdepim) suite helps you to organize your mail, tasks, appointments, and contacts.

This update includes the following fix:

- kdepim.spec used "%{prefix}/share/doc" in the %install section but had no "Prefix:" header line. Consequently, the symlinks created in this section were not relative (contrary to the included comment). With this update "%{prefix}/share/doc" has been replaced with "%{_docdir}", ensuring the created symlinks are relative, as expected.

All kdepim users should upgrade to these updated packages, which resolve this issue.

1.110. kernel

1.110.1. RHSA-2010:0147: Important security and bug fix update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2010:0147 .

Updated kernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 5.

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 in the References section.

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

Security fixes:

- a NULL pointer dereference flaw was found in the **`sctp_rcv_ootb()`** function in the Linux kernel Stream Control Transmission Protocol (SCTP) implementation. A remote attacker could send a specially-crafted SCTP packet to a target system, resulting in a denial of service. (CVE-2010-0008, Important)
- a missing boundary check was found in the **`do_move_pages()`** function in the memory migration functionality in the Linux kernel. A local user could use this flaw to cause a local denial of service or an information leak. (CVE-2010-0415, Important)
- a NULL pointer dereference flaw was found in the **`ip6_dst_lookup_tail()`** function in the Linux kernel. An attacker on the local network could trigger this flaw by sending IPv6 traffic to a target system, leading to a system crash (kernel OOPS) if ***`dst->neighbour`*** is NULL on the target system when receiving an IPv6 packet. (CVE-2010-0437, Important)

- a NULL pointer dereference flaw was found in the ext4 file system code in the Linux kernel. A local attacker could use this flaw to trigger a local denial of service by mounting a specially-crafted, journal-less ext4 file system, if that file system forced an EROFS error. (CVE-2009-4308, Moderate)
- an information leak was found in the **`print_fatal_signal()`** implementation in the Linux kernel. When **`/proc/sys/kernel/print-fatal-signals`** is set to 1 (the default value is 0), memory that is reachable by the kernel could be leaked to user-space. This issue could also result in a system crash. Note that this flaw only affected the i386 architecture. (CVE-2010-0003, Moderate)
- missing capability checks were found in the ebtables implementation, used for creating an Ethernet bridge firewall. This could allow a local, unprivileged user to bypass intended capability restrictions and modify ebtables rules. (CVE-2010-0007, Low)

Bug fixes:

- a bug prevented Wake on LAN (WoL) being enabled on certain Intel hardware. (BZ#543449)
- a race issue in the Journaling Block Device. (BZ#553132)
- Prior to this update, user data corruption could occur when a 64-bit system was in the 32-bit compatibility mode. Specifically, programs compiled on an x86 system that called **`sched_rr_get_interval()`** were silently corrupted. This was due to the kernel filling data beyond the end of a timespec structure because the size of the structure is different between 32-bit and 64-bit systems. With this update, this issue has been fixed by calling **`sys32_sched_rr_get_interval()`** instead of **`sys_sched_rr_get_interval()`** when **`sched_rr_get_interval()`** is called, and user data corruption no longer occurs. (BZ#557684)
- the RHSA-2010:0019 update introduced a regression, preventing WoL from working for network devices using the e1000e driver. (BZ#559335)
- adding a bonding interface in mode balance-alb to a bridge was not functional. (BZ#560588)
- some KVM (Kernel-based Virtual Machine) guests experienced slow performance (and possibly a crash) after suspend/resume. (BZ#560640)
- on some systems, VF cannot be enabled in **`dom0`**. (BZ#560665)
- on systems with certain network cards, a system crash occurred after enabling GRO. (BZ#561417)
- for x86 KVM guests with pvclock enabled, the boot clocks were registered twice, possibly causing KVM to write data to a random memory area during the guest's life. (BZ#561454)
- serious performance degradation for 32-bit applications, that map (**`mmap`**) thousands of small files, when run on a 64-bit system. (BZ#562746)
- improved kexec/kdump handling. Previously, on some systems under heavy load, kexec/kdump was not functional. (BZ#562772)
- **`dom0`** was unable to boot when using the Xen hypervisor on a system with a large number of logical CPUs. (BZ#562777)
- a fix for a bug that could potentially cause file system corruption. (BZ#564281)
- a bug caused infrequent cluster issues for users of GFS2. (BZ#564288)
- **`gfs2_delete_inode`** failed on read-only file systems. (BZ#564290)

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.

1.110.2. RHSA-2009:1193: Important security and bug fix update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1193

Updated kernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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

Security fixes:

- the possibility of a timeout value overflow was found in the Linux kernel high-resolution timers functionality, hrtimers. This could allow a local, unprivileged user to execute arbitrary code, or cause a denial of service (kernel panic). (CVE-2007-5966, Important)
- a flaw was found in the Intel PRO/1000 network driver in the Linux kernel. Frames with sizes near the MTU of an interface may be split across multiple hardware receive descriptors. Receipt of such a frame could leak through a validation check, leading to a corruption of the length check. A remote attacker could use this flaw to send a specially-crafted packet that would cause a denial of service or code execution. (CVE-2009-1385, Important)
- Michael Tokarev reported a flaw in the Realtek r8169 Ethernet driver in the Linux kernel. This driver allowed interfaces using this driver to receive frames larger than could be handled, which could lead to a remote denial of service or code execution. (CVE-2009-1389, Important)
- the ADDR_COMPAT_LAYOUT and MMAP_PAGE_ZERO flags were not cleared when a setuid or setgid program was executed. A local, unprivileged user could use this flaw to bypass the mmap_min_addr protection mechanism and perform a NULL pointer dereference attack, or bypass the Address Space Layout Randomization (ASLR) security feature. (CVE-2009-1895, Important)
- Ramon de Carvalho Valle reported two flaws in the Linux kernel eCryptfs implementation. A local attacker with permissions to perform an eCryptfs mount could modify the metadata of the files in that eCrypfts mount to cause a buffer overflow, leading to a denial of service or privilege escalation. (CVE-2009-2406, CVE-2009-2407, Important)
- Konstantin Khlebnikov discovered a race condition in the ptrace implementation in the Linux kernel. This race condition can occur when the process tracing and the process being traced participate in a core dump. A local, unprivileged user could use this flaw to trigger a deadlock, resulting in a partial denial of service. (CVE-2009-1388, Moderate)

Bug fixes:

- possible host (dom0) crash when installing a Xen para-virtualized guest while another para-virtualized guest was rebooting. (BZ#497812)
- no audit record for a directory removal if the directory and its subtree were recursively watched by an audit rule. (BZ#507561)
- page caches in memory can be freed up using the Linux kernel's drop_caches feature. If ***`drop_pagecache_sb()`*** and ***`prune_icache()`*** ran concurrently, however, a missing test in drop_pagecache_sb() could cause a kernel panic. For example, running **`echo 1 > /proc/sys/vm/drop_caches`** or **`sysctl -w vm.drop_caches=1`** on systems under high memory

load could cause a kernel panic or system hang. With this update, the missing test has been added and the drop_caches feature frees up page caches properly. Consequently these system failures no longer occur, even under high memory load. (BZ#503692)

- on 32-bit systems, core dumps for some multithreaded applications did not include all thread information. (BZ#505322)
- a stack buffer used by get_event_name() was not large enough for the nul terminator sprintf() writes. This could lead to an invalid pointer or kernel panic. (BZ#506906)
- when using the aic94xx driver, a system with SATA drives may not boot due to a bug in libsas. (BZ#506029)
- incorrect stylus button handling when moving it away then returning it to the tablet for Wacom Cintiq 21UX and Intuos tablets. (BZ#508275)
- CPU "soft lockup" messages and possibly a system hang on systems with certain Broadcom network devices and running the Linux kernel from the kernel-xen package. (BZ#503689)
- on 64-bit PowerPC, getitimer() failed for programs using the ITIMER_REAL timer and that were also compiled for 64-bit systems (this caused such programs to abort). (BZ#510018)
- write operations could be blocked even when using O_NONBLOCK. (BZ#510239)
- enabling MSI on systems with VIA VT3364 chipsets caused a kernel panic or system hang during installation of Red Hat Enterprise Linux or subsequent booting of the operating system. MSI was enabled by default during boot and the "pci=nomsi" boot option to disable MSI was required on Red Hat Enterprise Linux 5.2 and later to avoid this bug. With this update, the kernel automatically disables MSI on VIA VT3364 chipsets during boot. The "pci=nomsi" boot option is no longer required to install or boot Red Hat Enterprise Linux successfully. (BZ#507529)
- shutting down, destroying, or migrating Xen guests with large amounts of memory could cause other guests to be temporarily unresponsive. (BZ#512311)

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.

1.110.3. RHBA-2009:1151: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1151

Updated kernel packages that fix an issue with HugeTLBfs are now available for Red Hat Enterprise Linux 5.

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

These updated kernel packages fix the following bug:

- HugeTLBFS (Translation Look-Aside Buffer File System) allows much larger page sizes than standard 4-kilobyte pages. The kernel's virtual memory subsystem uses these pages to map between real and virtual memory address spaces, and HugeTLBFS allows for significant performance increases for memory-intensive applications under heavy load. When a file existing on the HugeTLB file system was accessed simultaneously by two separate processes, the system become unresponsive and eventually a soft lockup occurred. These updated packages correct this issue so that simultaneous access of a single file on a HugeTLB file system is no longer problematic. (BZ#510235)

Red Hat Enterprise Linux 5 users are advised to upgrade to these updated packages, which resolve these issues.

1.110.4. RHBA-2009:1133: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1133

Updated kernel packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

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

These updated packages addresses the following bugs:

- RHSA-2009-1106 included a fix for a rare race condition (BZ#486921). This earlier race condition occurred if an application performed multiple O_DIRECT reads per virtual memory page and also performed fork(2). Unfortunately, the fix included with RHSA-2009-1106 introduced a new, very small, race condition which presented if the system was swapping heavily or heavily reproducing the conditions that were the cause of BZ#48692. With this update, the parent pte is not set to writable if the src pte is unmapped by the VM, preventing the race condition from occurring. (BZ#507297)

- the copy_hugetlb_page_range() function assumed it was safe to drop the source mm->page_table_lock before calling hugetlb_cow(). As a consequence a kernel panic occurred when a particular multi-threaded application did Direct IO on a HUGEPAGE-mapped file region and created new processes. With this update, copy_hugetlb_page_range() calls hugetlb_cow() with the locks held, ensuring the panic does not occur. (BZ#508030)

Red Hat Enterprise Linux 5 users are advised to upgrade to these updated packages, which resolve these issues.

1.110.5. RHSA-2009:1106: Important security and bug fix update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1106

Updated kernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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

Security fixes:

- several flaws were found in the way the Linux kernel CIFS implementation handles Unicode strings. CIFS clients convert Unicode strings sent by a server to their local character sets, and then write those strings into memory. If a malicious server sent a long enough string, it could write past the end of the target memory region and corrupt other memory areas, possibly leading to a denial of service or privilege escalation on the client mounting the CIFS share. (CVE-2009-1439, CVE-2009-1633, Important)

- the Linux kernel Network File System daemon (nfsd) implementation did not drop the CAP_MKNOD capability when handling requests from local, unprivileged users. This flaw could possibly lead to an information leak or privilege escalation. (CVE-2009-1072, Moderate)
- Frank Filz reported the NFSv4 client was missing a file permission check for the execute bit in some situations. This could allow local, unprivileged users to run non-executable files on NFSv4 mounted file systems. (CVE-2009-1630, Moderate)
- a missing check was found in the hypervisor_callback() function in the Linux kernel provided by the kernel-xen package. This could cause a denial of service of a 32-bit guest if an application running in that guest accesses a certain memory location in the kernel. (CVE-2009-1758, Moderate)
- a flaw was found in the AGPGART driver. The agp_generic_alloc_page() and agp_generic_alloc_pages() functions did not zero out the memory pages they allocate, which may later be available to user-space processes. This flaw could possibly lead to an information leak. (CVE-2009-1192, Low)

Bug fixes:

- a race in the NFS client between destroying cached access rights and unmounting an NFS file system could have caused a system crash. "Busy inodes" messages may have been logged. (BZ#498653)
- nanosleep() could sleep several milliseconds less than the specified time on Intel Itanium®-based systems. (BZ#500349)
- LEDs for disk drives in AHCI mode may have displayed a fault state when there were no faults. (BZ#500120)
- ptrace_do_wait() reported tasks were stopped each time the process doing the trace called wait(), instead of reporting it once. (BZ#486945)
- epoll_wait() may have caused a system lockup and problems for applications. (BZ#497322)
- missing capabilities could possibly allow users with an fsuid other than 0 to perform actions on some file system types that would otherwise be prevented. (BZ#497271)
- on NFS mounted file systems, heavy write loads may have blocked nfs_getattr() for long periods, causing commands that use stat(2), such as ls, to hang. (BZ#486926)
- in rare circumstances, if an application performed multiple O_DIRECT reads per virtual memory page and also performed fork(2), the buffer storing the result of the I/O may have ended up with invalid data. (BZ#486921)
- when using GFS2, gfs2_quotad may have entered an uninterpretable sleep state. (BZ#501742)
- with this update, get_random_int() is more random and no longer uses a common seed value, reducing the possibility of predicting the values returned. (BZ#499783)
- the "-fwrapv" flag was added to the gcc build options to prevent gcc from optimizing away wrapping. (BZ#501751)
- a kernel panic when enabling and disabling iSCSI paths. (BZ#502916)
- using the Broadcom NetXtreme BCM5704 network device with the tg3 driver caused high system load and very bad performance. (BZ#502837)
- "/proc/[pid]/maps" and "/proc/[pid]/smaps" can only be read by processes able to use the ptrace() call on a given process; however, certain information from "/proc/[pid]/stat" and "/proc/[pid]/wchan" could be used to reconstruct memory maps. (BZ#499546)

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.

1.110.6. RHSA-2009:0473: Important security and bug fix update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0473

Updated kernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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

This update fixes the following security issues:

- a logic error was found in the do_setlk() function of the Linux kernel Network File System (NFS) implementation. If a signal interrupted a lock request, the local POSIX lock was incorrectly created. This could cause a denial of service on the NFS server if a file descriptor was closed before its corresponding lock request returned. (CVE-2008-4307, Important)
- a deficiency was found in the Linux kernel system call auditing implementation on 64-bit systems. This could allow a local, unprivileged user to circumvent a system call audit configuration, if that configuration filtered based on the "syscall" number or arguments. (CVE-2009-0834, Important)
- the exit_notify() function in the Linux kernel did not properly reset the exit signal if a process executed a set user ID (setuid) application before exiting. This could allow a local, unprivileged user to elevate their privileges. (CVE-2009-1337, Important)
- a flaw was found in the ecryptfs_write_metadata_to_contents() function of the Linux kernel eCryptfs implementation. On systems with a 4096 byte page-size, this flaw may have caused 4096 bytes of uninitialized kernel memory to be written into the eCryptfs file headers, leading to an information leak. Note: Encrypted files created on systems running the vulnerable version of eCryptfs may contain leaked data in the eCryptfs file headers. This update does not remove any leaked data. Refer to the Knowledgebase article in the References section for further information. (CVE-2009-0787, Moderate)
- the Linux kernel implementation of the Network File System (NFS) did not properly initialize the file name limit in the nfs_server data structure. This flaw could possibly lead to a denial of service on a client mounting an NFS share. (CVE-2009-1336, Moderate)

This update also fixes the following bugs:

- the enic driver (Cisco 10G Ethernet) did not operate under virtualization. (BZ#472474)
- network interfaces using the IBM eHEA Ethernet device driver could not be successfully configured under low-memory conditions. (BZ#487035)
- bonding with the "arp_validate=3" option may have prevented fail overs. (BZ#488064)
- when running under virtualization, the acpi-cpufreq module wrote "Domain attempted WRMSR" errors to the dmesg log. (BZ#488928)
- NFS clients may have experienced deadlocks during unmount. (BZ#488929)

- the ixgbe driver double counted the number of received bytes and packets. (BZ#489459)
- the Wacom Intuos3 Lens Cursor device did not work correctly with the Wacom Intuos3 12x12 tablet. (BZ#489460)
- on the Itanium® architecture, nanosleep() caused commands which used it, such as sleep and usleep, to sleep for one second more than expected. (BZ#490434)
- a panic and corruption of slab cache data structures occurred on 64-bit PowerPC systems when clvmd was running. (BZ#491677)
- the NONSTOP_TSC feature did not perform correctly on the Intel® microarchitecture (Nehalem) when running in 32-bit mode. (BZ#493356)
- keyboards may not have functioned on IBM eServer System p machines after a certain point during installation or afterward. (BZ#494293)
- using Device Mapper Multipathing with the qla2xxx driver resulted in frequent path failures. (BZ#495635)
- if the hypervisor was booted with the dom0_max_vcpus parameter set to less than the actual number of CPUs in the system, and the cpuspeed service was started, the hypervisor could crash. (BZ#495931)
- using Openswan to provide an IPsec virtual private network eventually resulted in a CPU soft lockup and a system crash. (BZ#496044)
- it was possible for posix_locks_deadlock() to enter an infinite loop (under the BKL), causing a system hang. (BZ#496842)

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.

1.110.7. RHSA-2009:0326: Important security and bug fix update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0326

Updated kernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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

Security fixes:

- memory leaks were found on some error paths in the icmp_send() function in the Linux kernel. This could, potentially, cause the network connectivity to cease. (CVE-2009-0778, Important)
- Chris Evans reported a deficiency in the clone() system call when called with the CLONE_PARENT flag. This flaw permits the caller (the parent process) to indicate an arbitrary signal it wants to receive when its child process exits. This could lead to a denial of service of the parent process. (CVE-2009-0028, Moderate)
- an off-by-one underflow flaw was found in the eCryptfs subsystem. This could potentially cause a local denial of service when the readlink() function returned an error. (CVE-2009-0269, Moderate)

- a deficiency was found in the Remote BIOS Update (RBU) driver for Dell systems. This could allow a local, unprivileged user to cause a denial of service by reading zero bytes from the image_type or packet_size files in "/sys/devices/platform/dell_rbu/". (CVE-2009-0322, Moderate)
- an inverted logic flaw was found in the SysKonnect FDDI PCI adapter driver, allowing driver statistics to be reset only when the CAP_NET_ADMIN capability was absent (local, unprivileged users could reset driver statistics). (CVE-2009-0675, Moderate)
- the sock_getsockopt() function in the Linux kernel did not properly initialize a data structure that can be directly returned to user-space when the getsockopt() function is called with SO_BSDCOMPAT optname set. This flaw could possibly lead to memory disclosure. (CVE-2009-0676, Moderate)
- the ext2 and ext3 file system code failed to properly handle corrupted data structures, leading to a possible local denial of service when read or write operations were performed on a specially-crafted file system. (CVE-2008-3528, Low)
- a deficiency was found in the libATA implementation. This could, potentially, lead to a local denial of service. Note: by default, the "/dev/sg*" devices are accessible only to the root user. (CVE-2008-5700, Low)

Bug fixes:

- a bug in aic94xx may have caused kernel panics during boot on some systems with certain SATA disks. (BZ#485909)
- a word endianness problem in the qla2xx driver on PowerPC-based machines may have corrupted flash-based devices. (BZ#485908)
- a memory leak in pipe() may have caused a system deadlock. The workaround in Section 1.5, Known Issues, of the Red Hat Enterprise Linux 5.3 Release Notes Updates, which involved manually allocating extra file descriptors to processes calling do_pipe, is no longer necessary. (BZ#481576)
- CPU soft-lockups in the network rate estimator. (BZ#481746)
- bugs in the ixgbe driver caused it to function unreliably on some systems with 16 or more CPU cores. (BZ#483210)
- the iwl4965 driver may have caused a kernel panic. (BZ#483206)
- a bug caused NFS attributes to not update for some long-lived NFS mounted file systems. (BZ#483201)
- unmounting a GFS2 file system may have caused a panic. (BZ#485910)
- a bug in ptrace() may have caused a panic when single stepping a target. (BZ#487394)
- on some 64-bit systems, notsc was incorrectly set at boot, causing slow gettimeofday() calls. (BZ#488239)
- do_machine_check() cleared all Machine Check Exception (MCE) status registers, preventing the BIOS from using them to determine the cause of certain panics and errors. (BZ#490433)
- scaling problems caused performance problems for LAPI applications. (BZ#489457)
- a panic may have occurred on systems using certain Intel WiFi Link 5000 products when booting with the RF Kill switch on. (BZ#489846)
- the TSC is invariant with C/P/T states, and always runs at constant frequency from now on. (BZ#489310)

All 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.

1.110.8. RHSA-2009:0264: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0264

Updated kernel packages that resolve several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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

This update addresses the following security issues:

- a memory leak in keyctl handling. A local user could use this flaw to deplete kernel memory, eventually leading to a denial of service. (CVE-2009-0031, Important)
- a buffer overflow in the Linux kernel Partial Reliable Stream Control Transmission Protocol (PR-SCTP) implementation. This could, potentially, lead to a denial of service if a Forward-TSN chunk is received with a large stream ID. (CVE-2009-0065, Important)
- a flaw when handling heavy network traffic on an SMP system with many cores. An attacker who could send a large amount of network traffic could create a denial of service. (CVE-2008-5713, Important)
- the code for the HFS and HFS Plus (HFS+) file systems failed to properly handle corrupted data structures. This could, potentially, lead to a local denial of service. (CVE-2008-4933, CVE-2008-5025, Low)
- a flaw was found in the HFS Plus (HFS+) file system implementation. This could, potentially, lead to a local denial of service when write operations are performed. (CVE-2008-4934, Low)

In addition, these updated packages fix the following bugs:

- when using the nfsd daemon in a clustered setup, kernel panics appeared seemingly at random. These panics were caused by a race condition in the device-mapper mirror target.
- the clock_gettime(CLOCK_THREAD_CPUTIME_ID,) syscall returned a smaller timespec value than the result of previous clock_gettime() function execution, which resulted in a negative, and nonsensical, elapsed time value.
- nfs_create_rpc_client was called with a "flavor" parameter which was usually ignored and ended up unconditionally creating the RPC client with an AUTH_UNIX flavor. This caused problems on AUTH_GSS mounts when the credentials needed to be refreshed. The credops did not match the authorization type, which resulted in the credops dereferencing an incorrect part of the AUTH_UNIX rpc_auth struct.
- when copy_user_c terminated prematurely due to reading beyond the end of the user buffer and the kernel jumped to the exception table entry, the rsi register was not cleared. This resulted in exiting back to user code with garbage in the rsi register.
- the hexdump data in s390dbf traces was incomplete. The length of the data traced was incorrect and the SAN payload was read from a different place then it was written to.
- when using connected mode (CM) in IPoIB on ehca2 hardware, it was not possible to transmit any data.
- when an application called fork() and pthread_create() many times and, at some point, a thread forked a child and then attempted to call the setpgid() function, then this function failed and returned and ESRCH

error value.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. Note: for this update to take effect, the system must be rebooted.

1.110.9. RHSA-2009:1222: Important security and bug fix update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1222

Updated kernel packages that fix two security issues and a bug are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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

These updated packages fix the following security issues:

- a flaw was found in the SOCKOPS_WRAP macro in the Linux kernel. This macro did not initialize the sendpage operation in the proto_ops structure correctly. A local, unprivileged user could use this flaw to cause a local denial of service or escalate their privileges. (CVE-2009-2692, Important)
- a flaw was found in the udp_sendmsg() implementation in the Linux kernel when using the MSG_MORE flag on UDP sockets. A local, unprivileged user could use this flaw to cause a local denial of service or escalate their privileges. (CVE-2009-2698, Important)

Red Hat would like to thank Tavis Ormandy and Julien Tinnes of the Google Security Team for responsibly reporting these flaws.

These updated packages also fix the following bug:

- in the dlm code, a socket was allocated in tcp_connect_to_sock(), but was not freed in the error exit path. This bug led to a memory leak and an unresponsive system. A reported case of this bug occurred after running "cman_tool kill -n [nodename]". (BZ#515432)

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.

1.110.10. RHSA-2009:1243

Updated kernel packages that fix 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 5.

1.110.10.1. General Kernel Support

An outline of general kernel updates.

- KVM **`guest-smp tlb`** flushing without **`mmu-notifiers`** could corrupt memory as a kernel-based virtual machine (KVM) may add pages to the kernel freelist while another **`vcpu`** may still be writing to them through guest mode. This update adds **`mmu-notifier`** support to the kernel and also corrects a bug found in an earlier patch wherein **`mm_struct`** was grown by existing drivers and caused a failed kABI

check. This bug has been corrected by using an index that resides in an unused padding hole to avoid expanding the structure size.(BZ#485718)

- Pointer and signed arithmetic overflow wrapping has not previously been defined in the Linux kernel. This could cause **GCC** (GNU C Compiler) to assume that wrapping does not occur and attempt to optimize the arithmetic that the kernel may require for overflow testing. This update adds the **`-fwrapv`** variable to **GCC `CFLAGS`** in order to define wrapping behavior.(BZ#491266)

- An issue of contention between processes vying for the same memory space in high end systems was recently identified by TPC-C (Transaction Processing Council) benchmarking. This update includes **`fast-gup`** patches which use direct IO and provide a significant (up to 9-10%) performance improvement. This update has been tested thoroughly and is used in the 5.4 kernel to improve scalability. For further information, see this article. (BZ#474913)

- A new parameter has been added to this kernel, allowing system administrators to change the maximum number of modified pages **`kupdate`** writes to disk per iteration each time it runs. **`/proc/sys/vm/max_writeback_pages`** defaults to ***`1024`*** or 4MB so that a maximum of 1024 pages get written out by each iteration of **`kupdate`**. (BZ#479079).

- A new option (**`CONFIG_TASK_IO_ACCOUNTING=y`**) has been added to kernel to assist in monitoring IO statistics per process. This assists with troubleshooting in a production environment. (BZ#461636)

- In previous kernels, back-up processes were deteriorating **DB2** server responsiveness. This was caused by **`/proc/sys/vm/dirty_ratio`** preventing processes writing to pagecache memory when more than half of the unmapped pagecache memory was dirty (even if **`dirty_ratio`** was set to 100%). A change made in this kernel update overrides this limiting behavior. Now, when the **`dirty_ratio`** is set to 100%, the system will no longer limit writing to pagecache memory. (BZ#295291)

- The **`rd_blocksize`** option found in the previous kernel's ramdisk driver was causing data corruption when using large ramdisks under a reasonable system load. This update removes this unnecessary option and resolves the data corruption issues. (BZ#480663)

- The function **`getrusage`** is used to examine the resource usage of a process. It is useful in diagnosing problems and gathering data on resource usage. However, in instances where a process was spawning child threads, **`getrusage`**'s results would be in incorrect as it would examine only the parent process and not interrogate its children. This update implements **`rusadge_thread`** to allow for accurate resource usage results in these instances. (BZ#451063)

- The header **`/usr/include/linux/futex.h`** would previously interfere with compiling C source code files, resulting in an error. This update includes a patch which corrects problematic kernel only definitions and resolves the compiling error. (BZ#475790)

- In previous kernels the kernel version was not identified in *panic* or *oops* output messages. This update adds the kernel version details to these outputs. (BZ#484403)

- During release 2.6.18, the kernel was configured to provide kernel-headers for the package **`glibc`**. That process caused various files to be improperly marked for inclusion. The **`serial_reg.h`** file was incorrectly marked and not included in the **`kernel_headers`** rpm. This, in turn, caused problems with building other rpms. This update adds the **`serial_reg.h`** file and corrects the problem. (BZ#463538)

- In some circumstances **`upcrund`**, the process manager in HP's **Unified Parallel C** (UPC) product, returned an ESRCH result and failed when calling **`setpgid()`** for a child process forked by a sub-thread. This update includes a patch to fix for this problem. (BZ#472433)

- Functionality has been added to **`sysrq-t`** to display backtrace information about running processes. This will assist in debugging hung systems. (BZ#456588)

1.110.10.2. Debugging

Updates specifically related to debugging tasks.

- Independent software vendors and developers often use **hugepage** to avoid unnecessary memory reclaim. The previous kernel didn't take **coredump** from **hugepage** area. This made the debugging of software difficult. This update includes a feature to assist debugging by making the kernel take a **hugepage coredump**. (BZ#470411)
- This update includes a feature addition to recover kernel panic messages. The option **-M** has been added to the **makedumpfile** command which allows a user to dump **dmesg** log data from **vmcore** into a user-specified log file (**makedumpfile -M /proc/vmcore /path/to/log/file**). (BZ#485308)
- In this update various tracepoints have been implemented as a "Technology Preview". These interfaces add static probe points into the kernel subsystem such as 'Page Cache', 'NFS' and 'Networking' stack, for use with tools such as SystemTap. (Bugzilla #493444, #499008, #493454, #475719)
- This kernel update adds the '**success**' value to **sched_wakeup** and **sched_wakeup_new** tracepoints to track successful schedule wakes. (BZ#497414)
- This update includes a new **dropstat** script to monitor and locate packets that are dropped within the host machine. (BZ#470539)
- The new **systemtap** direct kernel tracepoint support requires access to the **trace/*.h** header files within the kernel-devel package. This update includes **/trace/*.h** headers in the **kernel-devel** package. (BZ#489096)

1.110.10.3. Security

Updates specifically related to security concerns.

- This update increases the maximum length of the kernel key field from the arbitrary 32 character length set in previous kernels to 255 characters. (BZ#475145)
- In keeping with Federal Information Processing Standardization 140 (FIPS140) certification requirements, this update includes:
  - Self-testing for; **ansi_cprng** (BZ#497891), **ctr(aes)** mode (BZ#497888), **Hmac-sha512** (BZ#499463) and **rfc4309(ccm(aes))** (BZ#472386).
  - Code to produce a signature file that **GRUB** performs a checksum against during the boot process. (BZ#444632)
  - Code to change the DSA key from 512 bit to 1024 bit for module signing. (BZ#413241)

1.110.10.4. Filesystems

Filesystem Updates.

- Support for the **FIEMAP** file extent mapping system has been included in this kernel update. (BZ#296951)
- The **ext4** file system code (included in Red Hat Enterprise Linux as a Technology Preview) was rebased for this release. (BZ#485315)
- This kernel update corrects performance issues with the Common Internet File System (**CIFS**) (a protocol that defines a standard for remote file access) including difficulties mounting certain Windows file systems or symlink files. (BZ#465143)

- Kernel support for the **XFS** high-performance file system has been added to this Red Hat Enterprise Linux release. In this initial implementation the functionality is limited to specific customers on a use-case basis. (BZ#470845)
- This release includes kernel support for the **FUSE** userspace file system. (BZ#457975)
- Tunable parameters that control the number of **NFSD** socket connections have been added to this kernel release. TCP connections have previously been capped at 80, regardless of the number of NFS threads that were open. (BZ#468092)
- This kernel update includes **FIEMAP** support for]**GFS2** (Global FIle System). (BZ#476626)
- This kernel update adds a **UUID** (Universal Unique IDentifier) field to the file system super block. (BZ#242696)
- This update includes a patch to allow access to files on a **GFS2** file system from client machines running the older (and previously incompatible) NFS v2 file sharing protocol. (BZ#497954)

1.110.10.5. Networking

Kernel updates that relate to Networking issues

- A new module has been added to this kernel version to enable **DSCP** (Differentiated Services Code Point) setting in systems using IPv6 netfilter. (BZ#481652)
- In order to boost virtualization performance on 10 Gigabyte Ethernet cards (and 10GbE performance in general), Generic Receive Offload (GRO) support (analogous to GSO support on egress) has been added to the IPv4 and IPv6 protocols in this kernel release. (BZ#499347)
- This kernel update includes new code to improve UDP port randomization. Previous versions of the randomization code could allow a security weakness by providing sub-optimal randomizing, as well as producing CPU drag while scanning for port numbers. This update corrects these behaviors. (BZ#480951)
- When using **setsockopt()** with option ***IPV6_MULTICAST_IF*** and ***optval*** set to ***0***, the previous kernel would return a result of **ENODEV**. This release updates ***setsockopt(IPV6_MULTICAST_IF)*** to report the correct value and not the error. (BZ#484971)
- This update includes numerous critical fixes for the NetXen device driver. These patches have been tested and implemented in the kernel upstream. A complete list of the changes and their effects can be found at BZ#485381.

1.110.10.6. General Platform Support

Platform support updates:

- ACPI Performance and Throttling state (P- and T-state) change notifications were not being handled correctly by the **OSPM** (Operating System-directed Power Management) driver. This affected the Intel® Node Manager's ability to monitor and manage CPU power usage. The kernel's **processor_core** code has been update to correct this issue. (BZ#487567)
- Problems were encountered with the Lenovo X61 (and other laptops which have a docking station with a CD/DVD drive); if the machine was undocked after a CD/DVD had been mounted in the docking station optical drive it would not be present when the machine was re-docked. The docking driver has been updated in this release to correct the problem. (BZ#485181)

1.110.10.7. Architecture Specific Support

Updates specific to particular computer architectures.

1.110.10.7.1. i386

Kernel updates for i386 architectures.

- In a virtual environment, timekeeping for Red Hat Enterprise Linux 64-bit kernels can be problematic, since time is kept by counting timer interrupts. De- and re-scheduling the virtual machine can cause a delay in these interrupts, resulting in a timekeeping discrepancy. This kernel release reconfigures the timekeeping algorithm to keep time based on a time-elapsed counter. (BZ#463573)
- It was found that, if their stacks exceed the combined size of ~4GB, 64-bit threaded applications slowed down drastically in **`pthread_create()`**. This is because **`glibc`** uses **`MAP_32BIT`** to allocate those stacks. As the use of **`MAP_32BIT`** is a legacy implementation, this update adds a new flag (**`MAP_STACK mmap`**) to the kernel to avoid constraining 64-bit applications. (BZ#459321)
- The update includes a feature bit that encourages Time Stamp Clocks (TSCs) to keep running in deep-C states. This bit **`NONSTOP_TSC`** acts in conjunction with **`CONSTANT_TSC`**. **`CONSTANT_TSC`** indicates that the TSC runs at constant frequency irrespective of P/T- states, and **`NONSTOP_TSC`** indicates that TSC does not stop in deep C-states. (BZ#474091)
- This update includes a patch to include ***`asm-x86_64`*** headers in **`kernel-devel`** packages built on or for i386, i486, i586 and i686 architectures. (BZ#491775)
- This update includes a fix to ensure that specifying **`memmap=X$Y`** as a boot parameter on i386 architectures yields a new BIOS map. (BZ#464500)
- This update adds a patch to correct a problem with the Non-Maskable Interrupt (NMI) that appeared in previous kernel releases. The problem appeared to affect various Intel® processors and caused the system to report the NMI watchdog was 'stuck'. New parameters in the NMI code correct this issue. (BZ#500892)
- This release re-introduces PCI Domain support for HP **`xw9400`** and **`xw9300`** systems. (BZ#474891)
- Functionality has been corrected to export module **`powernow-k8`** parameters to **`/sys/modules`**. This information was previously not exported.(BZ#492010)

1.110.10.7.2. x86_64

Kernel updates for x86_64 architectures.

- An optimization error was found in **`linux-2.6-misc-utrace-update.patch`**. When running 32-bit processes on a 64-bit machine systems didn't return ENOSYS errors on missing (out of table range) system calls. This kernel release includes a patch to correct this. (BZ#481682)
- Some cluster systems where found to boot with an unstable time source. It was determined that this was a result of kernel code not checking for a free performance counter (**`PERFCTR`**) when calibrating the TSC (Time Stamp Clock) during the boot process. This resulted, in a small percentage of cases, in the system defaulting to a busy **`PERFCTR`** and getting unreliable calibrations.

  A fix was implemented to correct this by ensuring the system checked for a free ***`PERFCTR`*** before defaulting (BZ#467782). This fix, however, cannot satisfy all possible contingencies as it is possible that all ***`PERFCTR`***s will be busy when required for TSC calibration. Another patch has been included to initiate a kernel panic in the unlikely event (fewer than 1% of cases) that this scenario occurs. (BZ#472523).

1.110.10.7.3. PPC

Kernel updates for PowerPC architectures.

- This kernel release includes various patches to update the **spufs** (Synergistic Processing Units file system) for Cell processors. (BZ#475620)
- An issue was identified wherein **/proc/cpuinfo** would list logical PVR Power7 processor architecture as "unknown" when **show_cpuinfo()** was run. This update adds a patch to have **show_cpuinfo()** identify Power7 architectures as Power6. (BZ#486649)
- This update includes several patches that are required to add/improve **MSI-X** (Message Signaled Interrupts) support on machines using System P processors. (BZ#492580)
- A patch has been added to this release to enable the functionality of the previously problematic power button on Cell Blades machines. (BZ#475658)

1.110.10.7.4. S390

Kernel updates for S390 architectures.

- Utilizing Named Saved Segments (NSS), the z/VM hypervisior makes operating system code in shared real memory pages available to z/VM guest virtual machines. With this update, Multiple Red Hat Enterprise Linux guest operating systems on the z/VM can boot from the NSS and be run from a single copy of the Linux kernel in memory. (BZ#474646)
- Device driver support has been added in this update for the new IBM System z PCI cryptography accelerators, utilizing the same interfaces as prior versions. (BZ#488496)
- Control Program Identification (CPI) descriptive data is used to identify individual systems on the Hardware Management Console (HMC). With this update, CPI data can now be associated with a Red Hat Enterprise Linux instance. (BZ#475820)
- Fibre Channel Protocol (FCP) performance data can now be measured on Red Hat Enterprise Linux instances on the IBM System z platform. (BZ#475334). Metrics that are collected and reported n include:
  - Performance relevant data on stack components such as Linux devices, Small Computer System Interface (SCSI) Logical Unit Numbers (LUNs) and Host Bus Adapter (HBA) storage controller information.
  - Per stack component: current values of relevant measurements as throughput, utilization and other applicable measurements.
  - Statistical aggregations (minimum, maximum, averages and histogram) of data associated with I/O requests including size, latency per component and totals.
- Support has been added to the kernel to issue EMC Symmetrix Control I/O. This update provides the ability to manage EMC Symmetrix storage arrays with Red Hat Enterprise Linux on the IBM System z platform. (BZ#461288)
- Hardware that supports the configuration topology facility passes the system CPU topology information to the scheduler, allowing it to make load balancing decisions. On machines where I/O interrupts are unevenly distributed, CPUs that are grouped together and get more I/O interrupts than others will tend to have a higher average load, creating performance issues in some cases.

  Previously, CPU topology support was enabled by default. With this update, CPU topology support is disabled by default, and the kernel parameter "**topology=on**" has been added to allow this feature to be enabled.(BZ#475797)
- This update provides new kernel code to implement a client and server for a **TTY** (teletype) terminal server under z/VM using IUCV (Inter-User Communications Vehicle) as communication vehicle. Also, as part of this update, the **hvc_console** has been upgraded. (BZ#475551)

- This update includes functionality that allows users to add new kernel options using the IPL command without modifying the content of the CMS parmfile. The entire boot command line can be replaced with the VM parameter string and new Linux Named Saved Systems (NSS) can also be created on the CP/CMS command line. (BZ#475530)
- Crypto Device Driver use of Thin Interrupts (BZ#474700)
- This update adds a patch to configure shared kernel support via the **CONFIG_SHARED_KERNEL** parameter. (BZ#506947)

1.110.10.8. Miscellaneous Driver Updates

Details about driver updates.

- This release adds the final branding strings and the latest EagleLake graphics to the graphics driver (predominantly for the G41 chipset). (BZ#474513)
- This release updates the ALSA HDA audio driver to enable or improve support for new chipsets and HDA audio codecs. (BZ#483594)
- This update adds a new **EDAC** driver for Intel® **5000x** and **5400 MCH** processors. (BZ#462895)
- This release includes an updated version of the **SMBUS** (System Management Bus) driver that adds support for the AMD **SB800** series of products and improves handling of **SB400**, **SB600** and **SB700** products. (BZ#488746)
- A new PCI ID has been added to this release to enable support for the Broadcom® **HT1100** chipset. (BZ#474240)
- This kernel release incorporates a series of updates that add support for Chelsio® Communications' Terminator 3 Ethernet adapters. These changes include support for XRC queues and updates of the **cxgb3**, **iw_nes NES iWARP**, **mthca** and **qlgc_vnic** drivers, the **rdma** headers and SDP and SRP protocols to the OpenFabrics Enterprise Distribution (OFED) 1.4.1 versions. (BZ#476301)
- Support has been added for Mellanox ConnectX based 10GigE Ethernet cards. This support required updates of the **mlx4**, **mlx4_ib** and **mlx4_core** drivers as well as the inclusion of the hybrid **mlx4_en** driver. (BZ#477065 and BZ#456525)
- Problems with connectivity (using eHCA adapters) and various scripting issues have been rectified with updates to **eHCA** and **IPoIB** drivers in this release. (BZ#466086)
- Infiniband driver updates, incorporated with the OFED 1.4.1 release upgrade, have rectified kernel panic issues encountered when removing **ib_ipath** module while running HXT HCAs (BZ#230035). This upgrade also resolved failed **RDMA latencytest** and **perftest** processes run with QLogic IB. (BZ#480696)
- This update includes a patch that corrects a network port ordering problem encountered on systems using HP **ProLiant** or **xw460c** blade processors. (BZ#490068)
- A comprehensive series of patches have been included in this update to add and/or improve virtualization features. A complete list (including explanatory notes) can be found at BZ#493152.
- Several bugfixes and updates available for HP's Integrated Lights-Out (**hpilo**) product have been ported into this kernel release. A complete list can be found here; BZ#488964.

- PCI device drivers enable devices using **pci_enable()**, which enables regions probed by the device's Base Address Register (BAR). On larger servers I/O port resources may not be assigned to all the PCI devices due to coded limitations and base register fragmentation. This update adds, removes and refines multiple functions so as to improve resource allocation around free I/O ports. (BZ#442007)
- Three new patches have been added to this kernel to improve the passing of PCI devices between a virtual machine and its host. These patches first bind the device in question to a dummy driver (**pcistub.ko**) to prevent the host machine using it. Then, once the guest is finished with the device, **drivers_probe** prompts the kernel to re-load the true driver for that device and **remove_id** removes the relevant entry from the dynamic ID list. These new features operate successfully in both KVM and Xen virtualization environments. (BZ#491842)
- An updated driver for the Davicom **DM9601** Ethernet Adaptor has been included in this release. The new driver corrects previous unreliability using this device and other devices using the same chipset. (BZ#471800)
- This kernel release includes a patch to improve Huawei **EC121** USB 3G modem support. (BZ#485182)
- The driver for Apple Intel® hardware configurations (**efifb**) has been updated, providing various performance improvements when running this release on these machines. (BZ#488820)

1.110.10.9. Network Driver Updates

Updates to Network-related drivers:

- This update adds a feature to support bonding over **IPoIB** interfaces. A new **ib-bond** package has been added to the kernel to allow multiple link HA and improve load balancing and aggregation performance. (BZ#430758)
- Two new drivers (**cnic** and **bnx2i**) have been added to the kernel to introduce iSCSI support for Broadcom® **BNX2** and **BNX2x** Network Interface Cards (NICs). (BZ#441979)
- A new device driver **igbvf**) for **SR/IOV** enabled Intel® NICs has been added to this kernel release. This driver provides a significant performance improvement for virtualization using **SR/IOV** cards. (BZ#480524)
- Generic Receive Offload (GRO) support has been implemented in this update, both. The GRO system increases the performance of inbound network connections by reducing the amount of processing done by the Central Processing Unit (CPU). GRO implements the same technique as the Large Receive Offload (LRO) system, but can be applied to a wider range of transport layer protocols. GRO support has also been added to a several network device drivers, including the **igb** driver for Intel® Gigabit Ethernet Adapters and the **ixgbe** driver for Intel® 10 Gigabit PCI Express network devices. (BZ#499347)
- The **cxgb3** driver, which supports the Chelsio® 10Gb RNIC adapter, has been updated in order to enable iSCSI TOE support. (BZ#439518)
- This kernel updates the **enic** Cisco® 10Gi Ethernet driver to version 1.0.0.933. (BZ#484824)
- This kernel updates the Atheros® **ath5k** driver. This upgrade resolves a problem encountered by Atheros® users wherein the kernel reported an inability to wake up the MAC chip. Setting the call to **ath5k_set_pcie()** to execute earlier in the initialization process corrects this issue. (BZ#479049)
- Support for the Crystal Beach 3 I/O AT (Acceleration Technology) device has been included in this kernel update. (BZ#436039, BZ#436048)
- This update upgrades the **bnx2** driver for Broadcom® network devices. The update fixes multiple performance issues, including a kernel panic occurrence (when attempting to unload the driver while in use) and a non-responsiveness issue (caused by call-traces initiated by network certification processes).

(BZ#475567, BZ#476897, BZ#489519)

- This release updates the Broadcom® **bnx2x** driver to version 1.48.105. (BZ#475481)
- The **igb** driver has been updated to correct a stability issue (when encountered when setting the ***mtu*** parameter to less than 1K) and improve support for Intel® 82576 based devices. (BZ#484102, BZ#474881)
- In this update the bonding driver has been updated to the latest upstream version. This update, however has introduced **symbol/ipv6** module dependency capabilities. Therefore, if bonding has been previously disabled (by inserting the **install ipv6 /bin/false** line in the **/etc/modprobe.conf** file) this upgrade to the bonding driver will result in the bonding kernel module failing to load. The **install ipv6 /bin/false** line needs to be replaced with **install ipv6 disable=1** for the module to load properly. (BZ#462632)
- The **ixgbe** driver has been updated to version 2.0.8-k2 and support the 82599 (Niantic) device has been added. (BZ#472547)
- System freezes encountered when performing multiple remote copy programs to a system using the Nvidia® nForce chipset has been corrected by updating the **forcedeth** driver to version 0.62. (BZ#479740)
- The **sky2** Ethernet driver has been updated to support the Marvell® 88E8070 NIC. (BZ#484712)
- The **tg3** driver has been updated to version 3.96. This update corrects problems with sluggish performance (on systems with BCM5704 NICs) and adds full support for Broadcom® 5785 NICs. (BZ#481715 BZ#469772)

1.110.10.10. Storage Driver Updates

Driver updates for Storage devices

- The SCSI tape driver (st) has been enhanced with support for the Suppress Incorrect Length Indicator (SILI) bit in variable block mode. If SILI is set, reading a block shorter than the byte count does not result in **CHECK CONDITION**. The length of the block is determined using the residual count from the HBA. Avoiding the REQUEST SENSE command for every block speeds up some applications considerably. The SILI bit is set to off by default. It must only be set this if the tape drive supports SILI and the HBA correctly returns transfer residuals.

Note

The current version of the mt-st management utility does not have a keyword for the SILI bit. It must be set explicitly with:

```
mt -f /dev/nst0 stsetoptions 0x4000
```

BZ#457970.

- The **bnx2** driver now supports iSCSI. The **bnx2i** driver will access the **bnx2** driver through the **cnic** module to provide iSCSI offload support. (BZ#441979 and BZ#441979)

Note

The **bnx2i** version included in this release does not support IPv6.

- The **md** driver has been updated to provide support for *bitmap merging*. This feature eliminates the need for full resync when performing data replication. (BZ#481226)
- The **scsi** driver now includes the upstream **scsi_dh_alua** module. This adds explicit *asymmetric logical unit access* (ALUA) support with this release. To utilize the **scsi_dh_alua** module when using **dm-multipath**, specify **alua** as the **hardware_handler** type in **multipah.conf**. (BZ#482737)

Note

For EMC Clariion devices, using only **scsi_dh_alua** or **dm-emc** alone is supported. Using both **scsi_dh_alua** and **dm-emc** is not supported.

- A bug in the retry logic of the **scsi** driver is now fixed. This bug made it possible for some failovers to execute properly in multipathed environments.(BZ#489582)
- The **rdac_dev_list** structure now includes **md3000** and **md3000i** entries. This allows users to benefit from the advantages provided by the **iscsi_dh_rdac** module. (BZ#487293)
- This release includes the new **mpt2sas** driver. This driver supports the SAS-2 family of adapters from LSI Logic. SAS-2 increases the maximum data transfer rate from 3Gb/s to 6Gb/s.

  The **mpt2sas** driver is located in the **drivers/scsi/mpt2sas** directory, as opposed to the older **mpt** drivers that are located in **drivers/message/fusion** directory. (BZ#475665)
- The **aacraid** driver has now been updated to version 1.1.5-2461. This update applies several upstream fixes for bugs affecting queued scans, controller boot problems, and other issues. (BZ#475559)
- The **aic7xxx** driver now features an increased maximum I/O size. This allows supported devices (such as SCSI tape devices) to perform writes with larger buffers. (BZ#493448)
- The **cciss** driver has been updated to apply upstream fixes for bugs affecting memory BAR discovery, the **rebuild_lun_table** and the MSA2012 scan thread. This update also applies several configuration changes to **cciss**. (BZ#474392)
- The **fnic** driver has been updated to version 1.0.0.1039. This applies several upstream bug fixes, updates the **libfc** and **fcoe** modules, and adds a new module parameter that controls debug logging at runtime. (BZ#484438)
- The **ipr** driver now supports MSI-X interrupts. (BZ#475717)
- A bug that caused iSCSI iBFT installations to panic during disk formatting is now fixed. (BZ#436791). Also, a bug in the **iscsi_r2t_rsp struct** that caused kernel panics during iSCSI failovers in some multipathed environments is now fixed. (BZ#484455)
- The **lpfc** driver has been updated to version 8.2.0.48. This enables hardware support for upcoming OEM programs. (BZ#476738 and BZ#509010)
- The **MPT fusion** driver is now updated to version 3.04.07rh v2. This applies several bug fixes. (BZ#475455)

- The **megaraid_sas** driver is now updated to version 4.08-RH1. This update applies the following upstream enhancements and fixes (among others):(BZ#475574)
  - This update adds a polling mode to the driver.
  - A bug affecting supported tape drives is now fixed. With this release, the **pthru** timeout value is now set to the O/S layer timeout value for commands sent to tape drives.
- The **mvsas** driver is now updated to version 0.5.4. This applies several fixes and enhancements from upstream, and adds support for Marvell RAID bus controllers MV64460, MV64461, and MV64462. (BZ#485126)
- The **qla2xxx** driver has been updated to version 8.03.00.10.05.04-k, and now supports *Fibre Channel over Convergence Enhanced Ethernet* adapters. With this release, **qla2xxx** also applies several bug fixes from upstream, including: (BZ#471900, BZ#480204, BZ#495092, BZ#495094 and BZ#496126)
  - Discrepancies detected during **OVERRUN** handling on 4GB and 8GB adapters are now corrected.
  - All **vports** are now alerted of any asynchronous events.
  - A bug that caused kernel panics with the QLogic 2472 card is now fixed.
  - The **stop_firmware** command is no longer retried if the first attempt results in a times out.
  - The sector mask value is no longer based on the fixed **optrom** size.
  - A bug that caused frequent path failures during I/O on multipathed devices is now fixed. (BZ#244967)
  - The driver source code is now kABI-compliant.
  - **dcbx** pointers are now set to **NULL** after freeing memory.
- The **qla4xxx** driver now features improved driver fault recovery. This update fixes a bug in the driver that prevented adapter recovery if there were outstanding commands detected on the host adapter. (BZ#497478)

1.110.10.11. Miscellaneous Updates

- This update removes the **kfree** function from **kret_probelock**'s scope so as to avoid a deadlock that could occur if **kretprobe_flush_task()** probes the **kfree** function while holding **kretprobe_lock** spinlock. In addition, the **kprobe** functionality has been disallowed on the **atomic_notifier_call_chain** function to avoid numerous recursive faults occurring when it is called by **kprobe** after a re-entry. (BZ#210555)
- PCI devices would disappear in Xen Paravirtual guest system upon reboot or reset. This was identified as a problem with information about PCI devices being removed from **xenstore** before **xend** was able to create a configuration for the rebooted domain. Code has been amended in **xenbus.c** to correct this behavior. (BZ#233801)
- A kernel crash occurred when a Xen user specified the **mem=** (or **highmem=**) command via the command line on either the host or guest systems. This was caused by the array allocated to the **p2m** table being too small which resulted in a page fault during the subsequent **memcpy()**. This update decreases the memory reservation and only copies the appropriate number of entries into the **p2m** table.(BZ#240429)
- RAID 0, RAID 1, RAID 10 and RAID 5 configurations have previously set **q->merge_bvec_fn** (a functior that asks a device driver if the next vector entry will fit into a bio constructed by a process) in a way that rejects bios crossing its stripe. A device mapper will accept a bio that has two or more vector entries and a size equal to or less than a page that crosses a stripe boundary, but the underlying RAID device will not.

This update configures the device mapper to set a one-page maximum request size and set its own **q->merge_bvec_fn** to reject any bios with multiple vector entries that span more pages. This fix precludes the generation of bios that will be rejected by a **q->merge_bvec_fn** controlled by RAID 0, 1, 10 or 5. BZ#223947)

- This update includes numerous patches to enable Gigabyte pagetable support. (BZ#251982).
  - **0002-hugetlb-multiple-hstates-for-multiple-page-sizes.patch**
  - **0003-hugetlbfs-per-mount-huge-page-sizes.patch**
  - **0004-hugetlb-new-sysfs-interface.patch**
  - **0005-hugetlb-abstract-numa-round-robin-selection.patch**
  - **0006-mm-introduce-non-panic-alloc_bootmem.patch**
  - **0007-mm-export-prep_compound_page-to-mm.patch**
  - **0008-hugetlb-support-larger-than-MAX_ORDER.patch**
  - **0009-hugetlb-support-boot-allocate-different-sizes.patch**
  - **0010-hugetlb-printk-cleanup.patch**
  - **0011-hugetlb-introduce-pud_huge.patch**
  - **0012-x86-support-GB-hugepages-on-64-bit.patch**
  - **0013-x86-add-hugepagesz-option-on-64-bit.patch**
  - **0014-hugetlb-override-default-huge-page-size.patch**
- DCA (Direct Cache Access) is a method for warming the cache in the CPU. As part of Intel®'s I/OAT technology, it minimizes performance-limiting bottlenecks. This release updates the kernel I/O AT code and includes support for DCA for Intel®'s 82572 Gigabit Ethernet adapter family (BZ#252949)
- The early GFS2 (Global File System) versions contained two system processes, gfs2_glockd and gfs2_scand which were responsible for scanning the in-core glock structures and freeing them if they were unused.

  In this release these processes have been replaced by a shrinker which frees glocks based on cues from the VM system. This results in a better use of memory and better response to low memory conditions (reducing the likelihood of "out of memory" issues). As a side effect, this update reduces the processing load produced by GFS2 under certain workloads. (BZ#273001)
- In order to enable new features (as discussed in Bugzillas #252949 and #436048) I/O AT (Advanced Technology) code has been updated and problems with **kABI** breakages have been corrected. (BZ#273441)
- This update corrects code that produced bad mpa messages on the restoration or migration of para-virtualized guest system. (BZ#288511)
- Problems caused by Message Signaled Interrupts on Hyper-Transport based machines using (some) Nvidia cards have been resolved by porting an upstream driver. (BZ#290701)

- Some versions of pSeries firmware fail to set up a **dma-window** property for PCI slots that are unoccupied. As a result, the loop searching for this propery, in **iommu_dev_setup_pSeriesLP()**, can run to the end, resulting in a NULL pointer dereference later in the routine. This patch prevents the crash and prints a warning message. (BZ#393241)

- The existing 10 second delay waiting for frontend devices to connect was found to be insufficient under some load conditions. This update increases timeout for device connection on boot to 30 seconds. (BZ#396621)

- In previous kernels the **tuntap** device send path did not have any packet accounting. This meant that the user-space sender could pin down arbitrary amounts of kernel memory by continuing to send data to an end-point that was congested. This update adds packet accounting to the **tun** driver so that **virtio-net** gets congestion feedback which is necessary to prevent packet loss for protocols lacking congestion control (such as UDP) when used in a guest. (BZ#495863)

- This update adds the virtualization feature VT-d. This feature provides hardware support for directly assigning physical devices to Xen fully virtualized (HVM) guests or KVM guests. The principal benefit of the feature is to improve device access performance to be close to native speeds. Please refer to the Red Hat Knowledgebase before using PCI device assignment with this technology to avoid possible system instability issues. (BZ#500901)

  VT-d support is disabled by default. To enable VT-d one must add intel_iommu=on to the kernel commandline. Enabling VT-d is required to assign a host's PCI device to a KVM guest. (BZ#504363)

  Additionally, only the assignment of NIC devices from host to guest is supported. Assigning a block device (hard disk) to a guest is not supported. On hardware platforms that support IOMMU passthrough it is recommended to also use the **iommu=pt** kernel commandline option as this will improve the performance of I/O devices in the host. This parameter has no effect on performance for devices assigned to guests.

  When the iommu=pt mode, if a device is assigned to (and then de-assigned from) a guest, it can no longer be used in the host until the host has been rebooted. PCI hotplug devices can not be used in iommu=pt mode

- This update includes a fix for kernel panic encountered when attempting to run a **kdump** process on hardware virtual machine (HVM) in an ia64 architecture environment. (BZ#418591)

- This update corrects softlockup issues encountered when booting earlier kernel versions in a virtual environment and setting the clocksource to read from the system's Programmable Interval Timer (PIT). (BZ#427588)

- A problem identified with Xen kernels manifested with **meminfo** reporting an incorrect **LowTotal** of 4Tb. A patch applied to the driver alters how **highmem** pages are handled and corrects the error. (BZ#428892)

- When users set **LPFC HBA** storage to reset in a loop the system would attempt to rediscover **SCSI** devices and some of these processes would time-out. The issue was found to be code paths deleting **SCSI** devices without setting the device state to **SDEV_DEL**. A patch included in this update corrects this behavior(BZ#430170)

- The Xen kernel does not currently support the suspend functionality. A fix has been applied to this release to remove the "Suspend" option from graphical user interface menus. (BZ#430928)

- This update fixes a race condition when queuing incoming **iucv** messages by spreading the message queue spinlock in the **message_pending** callback across the entire callback function.This resolves the race condition and enhances system stability. (BZ#499626)

- This feature fixes **hexdump** data in **s390dbf** traces, allowing Red Hat Enterprise Linux to have complete registered state change notification (RSCN) traces (up to 1024 bytes). (BZ#470618)

- This update adds support for the **connlimit** module to limit to the number of TCP connections accepted by specific ports. This feature reduces the risk of incidental DoS scenarios.(BZ#483588)
- This update modifies the **DASDFMT** (Direct Access Storage Device ForMaT) command to operate in the same way as similar IBM tools (such as **CPFMTXA** for zLinux/VM and **ICKDSF** for MVS).. (BZ#484836)
- This feature includes stability enhancements to the CPU hotplug kernel module. (BZ#485412)
- When using previous x86_64 Xen kernels installed on Promise internal RAID disk the SuperTrak EX (**stex**) inbox-driver would fail, causing a kernel panic and failure to load. The cause was found to be the allocation of contiguous memory space. Relevant code sections have been rewritten to lower the amount of memory demanded by the driver (Note: This reduces the RAID Migration feature set). (BZ#486466)

Note

Lowering memory demands reduces the RAID Migration feature set.

- Infiniband driver updates, incorporated with the OFED 1.4.1 release upgrade, have rectified poor TCP transer rate performance when running Infiniband IPoIB in heterogeneous environments (that is, between Intel 32bit to PPC64bit or similar). (BZ#434779)
- This update adds support for machines using Intel®'s Calpella chipset. (BZ#438469)
- This update includes a patch to fix an interrupt storm (several thousand interrupts) encountered after boot with CD/DVD drive connected to IDE of Enterprise South Bridge 2 (ESB2). (BZ#438979)
- Pre-release testing has assessed the **ipr** and **iprutil** drivers as supporting the SAS paddle card on pBlade extensions. (BZ#439566)
- An upstream change to the **e1000** and **bnx2** driver removed the functionality to generate entropy, causing applications requesting random data from **/dev/random** to hang or produce an error message. This update reintroduces the functionality. (BZ#439898)
- Problems with **ioctl SG_IO** calls to tape devices failing have been resolved with an upstream patch that address this and numerous other **iscsi** module issues. (BZ#440411)
- An update in this release changes page locking code to avoid a deadlock between **mmap/munmap** and **journaling** (ext3). (BZ#445433)
- This kernel release includes a bug to correct a crash encountered when attempting to format a DVD in a system booted to run **libata** and **ata-piix** IDE accelerators. (BZ#446086)
- This update includes a fix to prevent para-virtualized guest systems crashing when run in a host machine with 64G RAM or more. (BZ#448115)
- Patches from the upstream kernel that improve **gettimeofday** performance on hypervisors have been incorporated in this release. With these changes serialization for **gettimeofday** is switched from CPUID to MFENCE/LFENCE. (BZ#448588)
- A bug that initiated a system reboot after a kernel panic despite **/proc/sys/kernel/panic** being set to ***-1*** (which should prevent a reboot) has been fixed in this update. (BZ#446120)
- Previous kernels were found to contain a bug that saw the **E1000** driver enable TSOv6 functionality for hardware that doesn't support it. A patch included in this update corrects this behavior.(BZ#449175)
- When booting fully virtualized guests on on earlier 32-bit kernel hosts, it was found that guest systems

with more than one virtual cpu could pause or even hang at the "starting udev" portion of the boot sequence. This bug was caused by one VCPU of an HVM guest missing timer ticks and Xen not re-delivering those missed ticks. This behavior caused a clock skew between VCPUs inside an HVM guest. These issues have been resolved with the backport of the AIO disk handling code and upstream Xen 'no missed-tick accounting' timer code. (BZ#449346)

- This update changes code that allowed **`scsi_add_host()`** to return a success even if the relevant **`work_q`** was not created. (BZ#450862)
- A bug in previous kernels allowed a **`ptrace`** process (**`ptrace(PTRACE_CONT, application_pid, 0, SIGUSR1`**) to terminate the specified application even if the **`SIGUSR1`** flag was blocked (which is sufficient to prevent a **`kill`** command from acting on the application). **`ptrace_induce_signal()`** is now used to set the blocked signal to pending, to be raised and executed only when the signal mask is cleared. (Bugzilla #451849)
- This update enables raw device support for IBM System z platforms. (Bugzilla #452534)
- This release updates the ext3 filesystem code to prevent kernel panic in dx_probe. (Bugzilla #454942)
- This kernel update removes the **`linux-2.6-ipmi-legacy-ioport-setup-changes.patch`** which was causing keyboard lockups (on IBM p-series, 7028 and 7029 models) during the installation process. (Bugzilla #455232)
- Messages being reported by **`zfcp`** testing processes have been removed from the message log in this kernel release. The tests in question were run when the local link was removed during heavy I/O loads, prompting **`zfcp`** to test remote ports. There is no need to include these details the message log as the tests cannot be influenced by a user and all relevant information is available using **`zfcp`** traces. (BZ#455260)
- This update removes the inclusion of the "Breaking affinity for irq XX" message in **`dmesg`** output. This message, reported when an **`XM migrate`** was performed, is not necessary and could negatively impact a user if observed in **`dmesg`** output. (BZ#456095)
- A patch has been included in this release to fix ACPI error flooding encountered when waking a Lenovo Thinkpad T61 (running the x86 kernel) from a suspended state. (BZ#456302)
- This release corrects how the **`powernow`** driver in the xen-kernel identifies the number of processors in guest systems. The original driver counted the number of processor *cores* in the machine causing it to identify dual-core processors as two distinct CPUs and return an incorrect processor count. (BZ#456437)

1.110.10.12. Further Updates

- Global File System 2 feature request improves performance of **`page_mkwrite()`**. (BZ#315191)
- A problem returning "Operation not supported" messages when setting an ACL from an NFSv4 system has been resolved. (BZ#403021)
- Fixes have been included in this release that prevent a kernel panic encountered when **`kprobes`** attempted boosting on exception addresses in x86_32 kernels. (BZ#493088)
- Various fixes and updates have been applied to the Xen Credit Scheduler and Xen Latency processes. (BZ#432700)
- An error encountered when attempting an online resize of an **`ext3`** filesystem using **`resize2fs`** is being investigated. The error returns "Invalid argument While trying to add group #15625" and can be avoided by doing resizes offline.(BZ#443541)

- This release included updated kernel code that resolves NFS connectathon test #12.1 problems. Processes are now called in a different scheduling order which avoids a race conflict. (BZ#448929)
- The **CPUID** driver has been updated to support **cpuid.4** and **cpuid.0xb** instruments. (Bugzilla #454981)
- This release contains an update to the **copy_user** code which fixes problems encountered when running **LTP read02** tests. (BZ#456682)
- Kernel code has been updated to fix an error in compiling a custom kernel that includes the **snd-sb16.ko** module. (BZ#456698)
- Various patches have been implemented in this release to resolve an issue with calltrace outputs showing on-screen during the shutdown of a Para-Virtualized domain. These outputs no longer appear during shutdown.(BZ#456893)
- An update in this release resolves system stalls that occurred when attempting to execute a **kdump** using the NMI key-combination. (BZ#456934)
- A patch has been applied to this kernel to prevent soft lockups occasionally encountered during boot on RX600S4 server systems. (BZ#456938)
- After booting from the HMC (load from file), it is now possible to reboot from an alternate device. (BZ#458115)

1.111. kexec-tools

1.111.1. RHBA-2009:0467: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0467

An updated kexec-tools package that fixes a bug is now available.

kexec-tools provides /sbin/kexec binary that allows a new kernel to boot using the kernel's kexec feature either on a normal or panic reboot. This package also contains the ancillary utilities that together form the user-space component of the kernel's kexec feature.

This updated kexec-tools package fixes the following bug:

- when kdump required mounting a file system which had reached its maximum mount count, fsck, the file system repair utility, was run automatically. However, because fsck was run in interactive mode by default, when it encountered a file system error the dump process paused until the user intervened. This prevented successful capture of the dump and subsequent system reboot. With this update, fsck is run in non-interactive mode, which allows the dump to complete successfully.

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

1.111.2. RHBA-2009:0048: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0048

An updated kexec-tools package that fixes a bug is now available

kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.

This updated package provides a fix for the following bug:

- Kernels booted under the kexec system failed to map regions in the system E820 map which were marked as reserved. As some hardware vendors use these regions for various configuration data, some systems experienced various failures during boot up. This update enables the mapping of all regions marked as reserved in the system E820 map and therefore allows these systems to boot correctly.

Users of kexec-tools should upgrade to this updated package, which resolves this issue.

1.111.3. RHBA-2009:1258: bug fix and enhancement update

An updated kexec-tools package that fixes various bugs and adds enhancements is now available.

kexec-tools provides the /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.

Bugs fixed in and enhancements added to this updated package include:

- the addition of reserved memory regions in kdump to improve booting on various systems. (BZ#475843)
- various other system-specific boot aids. (BZ#473730 , BZ#494782 and BZ#277531)
- a fix to handle network config files that are lacking an ending newline. (BZ#476063)
- improved the ability to detect md arrays. (BZ#479211 and BZ#490818)
- fixed some bad status messages when using the ssh dump target. (BZ#466450)
- fixed an issue in which sata_nv was not included in the initramfs. (BZ#476368)
- enhanced our dump filtering with the ability to dump dmesg logs. (BZ#475414)
- added a condrestart directive to the service initscript. (BZ#494483)
- updated the initramfs for kdump to use hostnames instead of ip addresses. (BZ#493690)
- cleaned up a few erroneous error messages. (BZ#496965 , BZ#506652 and BZ#509947)
- improved kdump documentation. (BZ#494473)
- fixed a bug in which kdump tried to unmount an un-mounted file system. (BZ#495601)
- improved kdump so that fsck operations were non-interactive. (BZ#497012)
- enhanced makedumpfile so that the utsname of the crashed kernel is saved in the dump header. (BZ#497021)

- fixed initrd generation to properly clean up files in /tmp. (BZ#483092)
- enhanced kdump to pickup virtio modules in use with kvm. (BZ#506863)
- made makedumpfile verbosity configurable. (BZ#466436)

Users should upgrade to this updated package, which resolves these issues.

1.112. krb5

1.112.1. RHSA-2009:0408: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0408

Updated krb5 packages that fix various security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third party, the Key Distribution Center (KDC). The Generic Security Service Application Program Interface (GSS-API) definition provides security services to callers (protocols) in a generic fashion. The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism is used by GSS-API peers to choose from a common set of security mechanisms.

An input validation flaw was found in the ASN.1 (Abstract Syntax Notation One) decoder used by MIT Kerberos. A remote attacker could use this flaw to crash a network service using the MIT Kerberos library, such as kadmind or krb5kdc, by causing it to dereference or free an uninitialized pointer. (CVE-2009-0846)

Multiple input validation flaws were found in the MIT Kerberos GSS-API library's implementation of the SPNEGO mechanism. A remote attacker could use these flaws to crash any network service utilizing the MIT Kerberos GSS-API library to authenticate users or, possibly, leak portions of the service's memory. (CVE-2009-0844, CVE-2009-0845)

All krb5 users should upgrade to these updated packages, which contain backported patches to correct these issues. All running services using the MIT Kerberos libraries must be restarted for the update to take effect.

1.112.2. RHBA-2009:1378: bug fix and enhancement update

Updated krb5 packages which fix several bugs and adds enhancements are now available for Red Hat Enterprise Linux 5.

Kerberos 5 is a network authentication system which authenticates clients and servers to each other using symmetric key encryption and a trusted third party, the KDC.

These updated packages address the following bugs:

- one of the error messages printed by the "ksu" command contained a spelling error ("geting"). This has been corrected. (BZ#462890)
- several dozen spelling errors across 21 krb5-related manual pages were corrected. (BZ#499190)

- this update no longer attempts to create a keytab for use by the kadmin service when the service is started; doing so is redundant and may interfere with third-party password-changing services such as those provided by IPA. (BZ#473151)
- with this update an attempt to load a database dump into a database which has not been created will cause kdb5_util to create the database. (BZ#442879)
- this update now correctly reports an error if an attempt to use rcp to copy data to a remote system encounters an error as the file is closed. (BZ#461902)

These new packages also add the following enhancements:

- the "ksu" command can now perform PAM account and session management for the target user. (BZ#477033)
- the Kerberos-aware rsh, rlogin, telnet, and ftp services can now set the PAM_RHOST item for users who log in or connect to a server remotely. (BZ#479071)

All users of the krb5 workstation utilities and services are advised to update to these packages which address these issues and add this enhancement.

1.113. ksh

1.113.1. RHBA-2009:1165: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1165

An updated ksh package that fixes a bug is now available.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with "sh", the original Bourne Shell.

This updated ksh package fixes the following bug:

- the ksh shell's "typeset" special builtin command allows scripts to perform nested variable assignment by providing a variable name and a value to assign to that variable name. However, when a ksh function which contained a nested variable was forked, the nesting counter was incorrectly set to zero, which caused nested variables assignments to become unset. This updated package corrects this error so that forked ksh functions have nested variables set correctly in their child processes, thus resolving the issue. (BZ#510712)

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

1.113.2. RHBA-2009:1256: bug fix update

Ksh package that fixes various bugs 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 includes fixes for the following bugs:

- when umask set a default permission in a subshell, this default permission would persist after returning to the parent shell. Subsequently, files in the parent shell might have been created with wrong permissions. This is now fixed. (BZ#485030)
- ksh removed variables from the environment if their names contained certain characters, for example, a hyphen or a space. Now, although ksh does not use environment variables with names that contain these characters, it keeps them for sub-processes. (BZ#488934)
- the ksh builtins failed to report errors on failed file operations, for example, if they were unable to write to a file because of no space on a disk. This could result in data loss, because a user would have no warning that data was not saved. Builtins now provide a proper return code and present an error message to the user if they are unable to complete a file operation. (BZ#465438)
- when typeset was used together with variable assignment in the last version of ksh, typeset took effect after the assignment, not before. Because this behavior was the opposite of how typeset works in ksh versions provided by pdksh and was not documented, it could create surprise and confusion. Now, ksh changed its behavior and typeset takes effect before the variable assignment. (BZ#489516)
- the ksh package now includes 'alternatives' which allows ksh switching with PDKSH. This feature allows users to switch between the ksh-93 and ksh-88 shells and to port ksh-88 scripts to ksh-93. (BZ#488798)
- ksh sometimes returned wrong OPTIND values after returning from a subshell when it executed a function within backquotes (backticks). While the original function would behave as expected, subseqeunt calls would result in incorrect OPTIND values, even calls made directly to the getopts function. Now, the use of backquotes does not cause ksh to return wrong OPTIND values on subsequent calls. (BZ#443889)
- the COMPATIBILITY file which describes differences between ksh-88 and ksh-93 has been added to %doc. (BZ#494534)
- if the $HISTFILE did not exist and could not be created for some reason (for example, read-only NFS home) ksh sometimes crashed with a segmentation fault when trying to insert the last word of the previous command using the M-_ or M-. keyboard shortcut. This is now fixed. (BZ#494363)
- the last version of ksh replaced the ast-base-locale language catalog with a ksh-specific language catalog. However, the ksh-specific catalog lacks translations for many of the locales shipped with ksh. Attempts to use ksh with a non-English locale would therefore result in error messages. Ksh now reverts to using the previous catalog, which does not produce these errors. (BZ#493570)
- in the last version of ksh, braces for a subscripted variable with ${var[sub]} became compulsory when inside [[...]], ((...)) or as a subscript. Because these braces were previouly optional, some shell scripts written for earlier versions of ksh no longer worked as expected. Ksh now recognises cases where the argument can be a pattern, and expands these variables the same way that it expanded them when the braces were optional. While this allows many old scripts to work in the current version of ksh, users cannot be certain that their scripts will work as expected unless they enclose variables in braces as defined in the ksh documentation. (BZ#498585)
- ksh now allows command history to be saved in global history file or in system log. (BZ#502747)
- in the last ksh version, the function nesting counter was zeroed after forking. Therefore, typeset did not assign values in asynchronously called functions. This is now fixed. (BZ#507562)

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

1.114. lcms

1.114.1. RHSA-2009:0339: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0339

Updated lcms packages that resolve several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Little Color Management System (LittleCMS, or simply "lcms") is a small-footprint, speed-optimized open source color management engine.

Multiple integer overflow flaws which could lead to heap-based buffer overflows, as well as multiple insufficient input validation flaws, were found in LittleCMS. An attacker could use these flaws to create a specially-crafted image file which could cause an application using LittleCMS to crash, or, possibly, execute arbitrary code when opened by a victim. (CVE-2009-0723, CVE-2009-0733)

A memory leak flaw was found in LittleCMS. An application using LittleCMS could use excessive amount of memory, and possibly crash after using all available memory, if used to open specially-crafted images. (CVE-2009-0581)

Red Hat would like to thank Chris Evans from the Google Security Team for reporting these issues.

All users of LittleCMS should install these updated packages, which upgrade LittleCMS to version 1.18. All running applications using the lcms library must be restarted for the update to take effect.

1.115. less

1.115.1. RHBA-2009:0413: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0413

An updated less package that fixes a bug is now available.

The less utility is a text file browser that resembles more, but with more capabilities ("less is more"). The less utility allows users to move backwards in the file as well as forwards. Because less need not read the entire input file before it starts, less starts up more quickly than text editors (vi, for example).

This updated less package fixes a bug which caused less to incorrectly add carriage return characters to the displayed output of text with lines which spanned longer than the terminal width. This could cause inconvenience when copying and pasting lines of text from a less session in the terminal. With this updated package, less no longer adds these carriage return characters, thus resolving the issue.

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

1.116. lftp

1.116.1. RHSA-2009:1278: Low security and bug fix update

An updated lftp package that fixes one security issue and various bugs is now available for Red Hat Enterprise Linux 5.

This update has been rated as having low security impact by the Red Hat Security Response Team.

LFTP is a sophisticated file transfer program for the FTP and HTTP protocols. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.

It was discovered that lftp did not properly escape shell metacharacters when generating shell scripts using the "mirror --script" command. A mirroring script generated to download files from a malicious FTP server could allow an attacker controlling the FTP server to run an arbitrary command as the user running lftp. (CVE-2007-2348)

This update also fixes the following bugs:

- when using the "mirror" or "get" commands with the "-c" option, lftp did not check for some specific conditions that could result in the program becoming unresponsive, hanging and the command not completing. For example, when waiting for a directory listing, if lftp received a "226" message, denoting an empty directory, it previously ignored the message and kept waiting. With this update, these conditions are properly checked for and lftp no longer hangs when "-c" is used with "mirror" or "get". (BZ#422881)

- when using the "put", "mput" or "reput" commands over a Secure FTP (SFTP) connection, specifying the "-c" option sometimes resulted in corrupted files of incorrect size. With this update, using these commands over SFTP with the "-c" option works as expected, and transferred files are no longer corrupted in the transfer process. (BZ#434294)

- previously, LFTP linked to the OpenSSL library. OpenSSL's license is, however, incompatible with LFTP's GNU GPL license and LFTP does not include an exception allowing OpenSSL linking. With this update, LFTP links to the GnuTLS (GNU Transport Layer Security) library, which is released under the GNU LGPL license. Like OpenSSL, GnuTLS implements the SSL and TLS protocols, so functionality has not changed. (BZ#458777)

- running "help mirror" from within lftp only presented a sub-set of the available options compared to the full list presented in the man page. With this update, running "help mirror" in lftp presents the same list of mirror options as is available in the Commands section of the lftp man page. (BZ#461922)

- LFTP imports gnu-lib from upstream. Subsequent to gnu-lib switching from GNU GPLv2 to GNU GPLv3, the LFTP license was internally inconsistent, with LFTP licensed as GNU GPLv2 but portions of the package apparently licensed as GNU GPLv3 because of changes made by the gnu-lib import. With this update, LFTP itself switches to GNU GPLv3, resolving the inconsistency. (BZ#468858)

- when the "ls" command was used within lftp to present a directory listing on a remote system connected to via HTTP, file names containing spaces were presented incorrectly. This update corrects this behavior. (BZ#504591)

- the default alias "edit" did not define a default editor. If EDITOR was not set in advance by the system, lftp attempted to execute "~/.lftp/edit.tmp.$$" (which failed because the file is not set to executable). The edit alias also did not support tab-completion of file names and incorrectly interpreted file names containing spaces. The updated package defines a default editor (vi) in the absence of a system-defined EDITOR. The edit alias now also supports tab-completion and handles file names containing spaces correctly for both downloading and uploading. (BZ#504594)

Note

This update upgrades LFTP from version 3.7.3 to upstream version 3.7.11, which incorporates a number of further bug fixes to those noted above. For details regarding these fixes, refer to the "/usr/share/doc/lftp-3.7.11/NEWS" file after installing this update. (BZ#308721)

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

1.117. libX11

1.117.1. RHEA-2009:1332: enhancement update

An enhanced libX11 package is now available.

libX11 is the X.Org X11 runtime library.

- The application would hang during SCIM key event handling, specifically when the user attempted to press the F4 key to change focus after typing Japanese characters in a text field. After that, it would not accept keyboard input.

  This was caused by a possible race condition between the client and the input method server.

  As a workaround, the number of available atoms for temporary storage of IM data has been increased. The F4 key should now allow the user to change focus most of the time. The frequency of this bug has been significantly reduced but be aware that it may still be triggered under certain circumstances. (BZ#437790)

- Fn+F? keys and System Buttons for Dell's Converse and Fila mobile platforms need to be mapped to appropriate actions. When pressed, nothing would happen. xkeyboard-config and libX11 have now been updated to accept input from these keys. These keys will now work when pressed. (BZ#496184)

User should upgrade to the updated package which adds these enhancements.

1.118. libdhcp

1.118.1. RHBA-2009:1333: bug fix update

Updated libdhcp packages that fix various bugs are now available.

libdhcp enables programs to invoke and control the Dynamic Host Configuration Protocol (DHCP) clients: the Internet Software Consortium (ISC) IPv4 DHCP client library, libdhcp4client, and the IPv6 DHCPv6 client library, libdhcp6client. libdhcp also provides network interface configuration services for network parameter auto-configuration with DHCP.

These updated libdhcp packages fix the following problems:

- libdhcp did not allow for some situations where a static network configuration was specified. Specifically, when a configuration without a DHCP server was specified during installation, the network interface was not activated. This would preclude installations through FTP and HTTP. Libdhcp now activates the interface when a static configuration is specified, even when no DHCP server is present so that network-based installations are possible. (BZ#233066)

- previously, the method used by libdhcp to build a list of network interfaces available on a system could accommodate a maximum of 86 interfaces. As a consequence, attempts to perform network-based

installations through interfaces eth86 and higher would fail. libdhcp now uses libnl to build a list of valid interfaces and therefore is no longer limited to the first 86 that it finds. Network-based installations are therefore possible on a wider range of hardware and network configurations. (BZ#444919)

Interfaces using static network configuration are properly handled during installation.

- The system will now see all available network interfaces in the system during installation, rather than stopping at eth85.

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

1.119. libgcrypt

1.119.1. RHEA-2009:1264: enhancement update

Updated libgcrypt packages that contain enhancements necessary for FIPS validation are now available.

The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.

This updated package rebases the libgcrypt library to version 1.4.4, the current upstream version. This rebase adds the following enhancements:

- runtime self-tests and FIPS mode setting have been added, both of which are necessary for Federal Information Processing Standards level 1 (FIPS 140-2) validation. Note: libgcrypt 1.4.4 is currently undergoing FIPS-140-2 validation. FIPS mode is disabled by default, however, to ensure the libgcrypt library maintains feature parity and ABI compatibility with libgcrypt packages previously included in Red Hat Enterprise Linux 5. The FIPS mode can be enabled with kernel command line setting or by creating an empty file, /etc/gcrypt/fips_enabled. (BZ#444803)

- libgcrypt now works with gnutls in non-enforced FIPS mode. (BZ#462718)

libgcrypt users are advised to upgrade to the updated packages, which provides these enhancements.

1.120. libpng

1.120.1. RHSA-2009:0333: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0333

Updated libpng and libpng10 packages that fix a couple of security issues are now available for Red Hat Enterprise Linux 2.1, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

A flaw was discovered in libpng that could result in libpng trying to free() random memory if certain, unlikely error conditions occurred. If a carefully-crafted PNG file was loaded by an application linked against libpng, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application. (CVE-2009-0040)

A flaw was discovered in the way libpng handled PNG images containing "unknown" chunks. If an application linked against libpng attempted to process a malformed, unknown chunk in a malicious PNG image, it could cause the application to crash. (CVE-2008-1382)

Users of libpng and libpng10 should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications using libpng or libpng10 must be restarted for the update to take effect.

1.121. libsemanage

1.121.1. RHBA-2009:1298: bug fix update

Updated libsemanage packages that fix multiple issues are now available.

libsemanage provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, as well as by programs such as load_policy, which must perform specific transformations on binary policies (for example, customizing policy boolean settings)

These updated packages fix the following bugs:

- dontaudit messages could not be disabled, which made it difficult for customers building their own security policies to identify which policies were being denied. This updated package includes the "sepol_set_disable_dontaudit" and "semanage_set_disable_dontaudit" functions, which allow dontaudit messages to be disabled. (BZ#493114)
- corrected a specific versioned dependency issue relating to libsepol (BZ#512662)

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

1.122. libsepol

1.122.1. RHBA-2009:1273: bug fix update

Updated libsepol packages that resolve several issues are now available.

libsepol provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, and programs such as load_policy, which must perform specific transformations on binary policies (for example, customizing policy boolean settings).

The updated libsepol packages address the following issues:

- the RPM package information specified that libsepol was provided under a GPL license. This contradicted the source RPM change log, which specified that libsepol was provided under a LGPL licence. The correct licence type (LGPL) is now specified in the libsepol package information. (BZ#488802)
- dontaudit messages could not be disabled, which made it difficult for customers building their own security policies to identify which policies were being denied. This updated package includes the "sepol_set_disable_dontaudit" function, which allows dontaudit messages to be disabled.

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

1.123. libsoup

1.123.1. RHSA-2009:0344: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0344

Updated libsoup and evolution28-libsoup packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

libsoup is an HTTP client/library implementation for GNOME written in C. It was originally part of a SOAP (Simple Object Access Protocol) implementation called Soup, but the SOAP and non-SOAP parts have now been split into separate packages.

An integer overflow flaw which caused a heap-based buffer overflow was discovered in libsoup's Base64 encoding routine. An attacker could use this flaw to crash, or, possibly, execute arbitrary code. This arbitrary code would execute with the privileges of the application using libsoup's Base64 routine to encode large, untrusted inputs. (CVE-2009-0585)

All users of libsoup and evolution28-libsoup should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running applications using the affected library function (such as Evolution configured to connect to the GroupWise back-end) must be restarted for the update to take effect.

1.124. libspe2

1.124.1. RHBA-2009:1263: bug fix and enhancement update

An updated libspe2 package (re-based to upstream version 2.3.0-135) is now available.

The SPE Runtime Management Library, libspe, provides the standardized low-level API for application access to the Cell Broadband Engine's Synergistic Processing Elements (SPEs). This API is neutral with respect to the underlying operating system and its SPE management methods.

This update re-bases the libspe 2.0 library to upstream version 2.3.0-135, which adds ADA bindings to support the ADA programming language and applies several bug fixes from upstream. (BZ#475619 and BZ#475637)

Users are advised to upgrade to this update.

1.125. libtiff

1.125.1. RHSA-2009:1159: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1159

Updated libtiff packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

Several integer overflow flaws, leading to heap-based buffer overflows, were found in various libtiff color space conversion tools. An attacker could create a specially-crafted TIFF file, which once opened by an unsuspecting user, would cause the conversion tool to crash or, potentially, execute arbitrary code with the privileges of the user running the tool. (CVE-2009-2347)

A buffer underwrite flaw was found in libtiff's Lempel-Ziv-Welch (LZW) compression algorithm decoder. An attacker could create a specially-crafted LZW-encoded TIFF file, which once opened by an unsuspecting user, would cause an application linked with libtiff to access an out-of-bounds memory location, leading to a denial of service (application crash). (CVE-2009-2285)

The CVE-2009-2347 flaws were discovered by Tielei Wang from ICST-ERCIS, Peking University.

All libtiff users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, all applications linked with the libtiff library (such as Konqueror) must be restarted for the update to take effect.

1.126. libunwind

1.126.1. RHBA-2009:0464: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0464

An updated libunwind package that removes the possibility of a crash when using unwinding capabilities is now available.

The libunwind package provides a portable C-based API for determining the call-chain of a program. In addition, libunwind makes it possible to manipulate the saved state of a call-frame, and resume execution at any call-chain point.

This updated libunwind package fixes the following bug:

- C++ programs which used standard C++ exceptions and were linked with the libunwind library could crash, due to a conflict between the unwinding capabilities contained in GCC and those provided by libunwind. libunwind used an outdated Application Binary Interface (ABI) which did not provide the GetIPInfo() function. When the libunwind unwinder was preferred over the GCC unwinder, then the missing GetIPInfo() function (which was provided by the GCC unwinder) was used together with libunwind's unwinding support. Because GCC's GetIPInfo() function must access the (valid) state of the GCC unwinder, an application crash could result. Because of this ABI change, libunwind required a small extension to its ABI to update it to the current unwinding ABI. This updated package provides that extension, thus removing the possibility for unwinding conflict and potential application crash. (BZ#480412)

Note: it is only necessary to update a system with these libunwind packages in order to avoid the potential application crash detailed above. It is not necessary to update any gcc packages.

All users who require unwinding capabilities are advised to upgrade to this updated package, which resolves this issue.

1.127. libvirt

1.127.1. RHSA-2009:0382: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0382

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

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

libvirt is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. libvirt also provides tools for remotely managing virtualized systems.

The libvirtd daemon was discovered to not properly check user connection permissions before performing certain privileged actions, such as requesting migration of an unprivileged guest domain to another system. A local user able to establish a read-only connection to libvirtd could use this flaw to perform actions that should be restricted to read-write connections. (CVE-2008-5086)

libvirt_proxy, a setuid helper application allowing non-privileged users to communicate with the hypervisor, was discovered to not properly validate user requests. Local users could use this flaw to cause a stack-based buffer overflow in libvirt_proxy, possibly allowing them to run arbitrary code with root privileges. (CVE-2009-0036)

All users are advised to upgrade to these updated packages, which contain backported patches which resolve these issues. After installing the update, libvirtd must be restarted manually (for example, by issuing a "service libvirtd restart" command) for this change to take effect.

1.127.2. RHEA-2009:1269: bug fix and enhancement update

Updated libvirt packages that upgrade the libvirt library to upstream version 0.6.3, add KVM hypervisor and PCI pass-through support, and fix a number of bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

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 5 to upstream version 0.6.3, which contains a large number of enhancements and bug fixes over the previous version. Importantly, with this libvirt update, Red Hat Enterprise Linux 5.4 is the first release to provide support for the KVM hypervisor. Also present in this update are PCI pass-through ability and PCI hot plug support. See the "enhancements" section below for details.(BZ#475821)

For a more complete list of changes and bug fixes in libvirt releases, refer to http://libvirt.org/news.html

These updated packages fix the following notable bugs:

- the "virsh" and "xm" commands passed incorrectly passed the option "type=vbd" when either attaching or detaching TAP devices, which caused the command to fail. With this update, the correct type, "type=tap", is passed when TAP devices are attached or detached. (BZ#475791)
- attempting to create a domain on a node using an iSCSI volume pool managed by libvirt failed with this error message:

```
libvir: Remote error : socket closed unexpectedly
error: Failed to create domain from create_guest.xml
```

This has been fixed in these updated packages so that creating guests on an iSCSI volume pool succeeds as expected. (BZ#483310)

- the "virsh" and "xm" commands passed incorrectly passed the option "type=vbd" when either attaching or detaching TAP devices, which caused the command to fail. With this update, the correct type, "type=tap", is passed when TAP devices are attached or detached. (BZ#483835)
- occasionally, libvirt lost track of running domains, the command "virsh list" did not list those domains, and pid files still existed for the processes representing those domains. A fix to the libvirt event loop now ensures that libvirt is able to keep track of all running domains on the host. (BZ#499250)
- due to a domain ID-handling error, the command "virsh destroy [domain-id]" could potentially terminate domains with IDs similar to the target. This has been corrected so that "virsh destroy [domain-id]" terminates only the target domain. (BZ#500158)
- running the command "virsh dominfo [domain-id]" to acquire information about a running Xen domain resulted in this error message:

```
error: this function is not supported by the hypervisor:
virNodeGetSecurityModel
```

This update fixes the dominfo subcommand so that it does not return an error message if the security model API is unimplemented. (BZ#506688)

- right-clicking on a running domain in the virt-manager application and then choosing Shutdown -> Force Off incorrectly caused that domain ID to disappear from the virt-manager list of VMs. In addition, domains created with the virt-manager or virt-install applications were not listed in the GUI window until virt-manager was restarted or the newly-created guest was started. This issue was related to inotify support and has been fixed in these updated packages. (BZ#508278)

In addition, these updated packages provide the following enhancements:

- PCI pass-through is a virtualization-related ability that is enabled by AMD's IOMMU and Intel's VT-d technologies. With PCI pass-through, PCI devices can be "passed through" the hypervisor (that is, bypassing it and locking it out) to an unprivileged domain, thereby allowing near-native performance of hardware devices, such as network cards, in guest domains. With this update, PCI pass-through is enabled for both Xen and KVM virtual machines. (BZ#471156 , BZ#513317 , BZ#496925 , BZ#481757 , BZ#481747)

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

1.128. libvirt-cim

1.128.1. RHEA-2009:1270: bug fix and enhancement update

An enhanced version of libvirt-cim which provides support for the KVM-based virtualization in Red Hat Enterprise Linux 5.4 is now available.

The introduction of KVM virtualization in Red Hat Enterprise Linux 5.4 required that libvirt-cim be rebased and updated to support the new hypervisor. Libvirt-cim is a CMPI CIM provider that lets you manage multiple platforms and provides support for some libvirt features.

This package applies the fix for the following bug:

- libvirt-cim would generate an incorrect boot tag for fully virtualized Xen guests, which would cause a 'Missing boot device' error. Boot tags will now generate in the form <boot dev='hd'> instead of <boot>hd</boot>, and guests will be able to start normally. (BZ#503724)

This package also adds the following enhancements:

- KVM virtualization in Red Hat Enterprise Linux, as mentioned above, requires an updated version of libvirt-cim to support the new hypervisor. libvirt-based CIM providers have been updated to enable support for third-party system management tools for Xen and KVM. (BZ#474681)
- Red Hat Enterprise Linux 4 introduced higher permission sensitivity to directory creation when installing packages. When the root's umask was changed prior to installation, and a package did not explicitly define directory permissions for a file, the installer would create directories based on the umask of the user who ran the installation. This could result in an 'Unowned Directory' error. libvirt-cim now includes full permission information, so directories are set up correctly during installation. (BZ#481810)

All users are advised to upgrade to this enhanced package, which resolves these issues.

1.129. libvorbis

1.129.1. RHSA-2009:1219: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1219

Updated libvorbis packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The libvorbis packages contain runtime libraries for use in programs that support Ogg Vorbis. Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format.

An insufficient input validation flaw was found in the way libvorbis processes the codec file headers (static mode headers and encoding books) of the Ogg Vorbis audio file format (Ogg). A remote attacker could provide a specially-crafted Ogg file that would cause a denial of service (memory corruption and application crash) or, potentially, execute arbitrary code with the privileges of an application using the libvorbis library when opened by a victim. (CVE-2009-2663)

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

1.130. libwmf

1.130.1. RHSA-2009:0457: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0457

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

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

libwmf is a library for reading and converting Windows Metafile Format (WMF) vector graphics. libwmf is used by applications such as GIMP and ImageMagick.

A pointer use-after-free flaw was found in the GD graphics library embedded in libwmf. An attacker could create a specially-crafted WMF file that would cause an application using libwmf to crash or, potentially, execute arbitrary code as the user running the application when opened by a victim. (CVE-2009-1364)

Note: This flaw is specific to the GD graphics library embedded in libwmf. It does not affect the GD graphics library from the "gd" packages, or applications using it.

Red Hat would like to thank Tavis Ormandy of the Google Security Team for responsibly reporting this flaw.

All users of libwmf are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, all applications using libwmf must be restarted for the update to take effect.

1.131. libxml

1.131.1. RHSA-2009:1206: Moderate and libxml2 security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1206

Updated libxml and libxml2 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

libxml is a library for parsing and manipulating XML files. 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.

A stack overflow flaw was found in the way libxml processes the root XML document element definition in a DTD. A remote attacker could provide a specially-crafted XML file, which once opened by a local, unsuspecting user, would lead to denial of service (application crash). (CVE-2009-2414)

Multiple use-after-free flaws were found in the way libxml parses the Notation and Enumeration attribute types. A remote attacker could provide a specially-crafted XML file, which once opened by a local, unsuspecting user, would lead to denial of service (application crash). (CVE-2009-2416)

Users should upgrade to these updated packages, which contain backported patches to resolve these issues. For Red Hat Enterprise Linux 3, they contain backported patches for the libxml and libxml2 packages. For Red Hat Enterprise Linux 4 and 5, they contain backported patches for the libxml2 packages. The desktop must be restarted (log out, then log back in) for this update to take effect.

1.132. linuxwacom

1.132.1. RHEA-2009:1384: enhancement update

New linuxwacom packages that provide new features are now available.

The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers

These updated packages include the following enhancements:

- serial tablets commonly found in tablet laptops were not recognized as tablets. The udev rules have been modified to create symbolic links, which adds serial tablet support. (BZ#483827)
- wacomcpl did not show a specific pointer device in the title bar of a submenu when a tool was edited. (That is, the title bar showed 'Tool Buttons' rather than 'Stylus Tool Buttons' when the Stylus tool was selected.) The device is now shown in the submenu title bar so that users can easily see which device is being edited. (BZ#485942)

Wacom tablet users who wish to use these features should upgrade to these new packages, which add the required support.

1.133. lksctp-tools

1.133.1. RHBA-2009:0412: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0412

Updated lksctp-tools packages that resolve several issues are now available.

These packages are intended to supplement the Stream Control Transmission Protocol (SCTP) reference implementation, which has been a part of the kernel since kernel version 2.5.36. For more information on LKSCTP see the section titled "LKSCTP - Linux Kernel SCTP" in the README file included in the package documentation. These packages contain the base runtime library and command line tools.

These updated lksctp-tools packages fix a memory leak related to socket manipulation in the sctp library. Also, explicit package version requirement was added into devel and doc sub-packages.

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

1.134. ltrace

1.134.1. RHBA-2009:0380: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0380

An updated ltrace package that fixes various bugs is now available.

The ltrace utility is a debugging program that runs a specified command until the command exits. While the command is executing, ltrace intercepts and records both the dynamic library calls called by the executed process and the signals received by the executed process. The ltrace utility can also intercept and print system calls executed by the process.

This updated ltrace package includes fixes for the following bugs:

- in some cases, when tracing the process that used fork system call, the kernel may have reported certain events in the forked child even before it reported that the fork had occurred in the first place. With this update, ltrace now anticipates this behavior, thus resolving the issue.
- on IBM System z machines, ltrace would crash when attempting to trace binaries that called functions with five or more arguments. This has been fixed with this update and ltrace now works as expected.
- when ltrace's '-o' option, which writes the output to a file, was used alongside the '-c' option, which counts time and calls for each library call and reports a summary, ltrace sent the output to standard error as usual instead of to the file designated on the command line. With this updated package, ltrace sends the output to the designated file when it is called with the '-c' option, thus resolving this issue.
- ltrace was not able to trace a binary that was called using the "exec" system call. With this update, ltrace is now able to do so.
- the ltrace(1) man page incorrectly claimed that ltrace could not trace 64-bit binaries, and has been corrected.
- a bug in which ltrace would become unresponsive (i.e. "hang") while tracing a child process with the '-f' option, which traces child processes as they are created by currently traced processes as a result of the fork or clone system calls. To correct for this, ltrace now tests for the situation in which it fails to attach to a newly-forked process, thus resolving the issue.

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

1.135. lvm2

1.135.1. RHBA-2009:1393: 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).

This update applies the following bug fixes:

- Fixes pvmove to revert operation if temporary mirror creation fails.
- Fixes metadata export for VG with missing PVs.
- Enables use of cached metadata for pvs and pvdisplay commands.
- Fixes segfault for vgcfgrestore on VG with missing PVs.

- Fixes memory leaks in toolcontext error path and mirror allocation code.
- Ignores suspended devices during repair and allows metadata correction even when PVs are missing.
- Unifies error messages when processing inconsistent volume group.
- Fixes multi-extent mirror log allocation when smallest PV has only 1 extent.
- Attempts to load dm-zero module if zero target needed but not present.
- Forces max_lv restriction only for newly created LV.
- Fixes vgreduce --removemissing failure exit code.
- Always returns exit error status when locking of volume group fails.
- Fixes mirror log convert validation question.
- Saves and restores the previous logging level when log level is changed internally.
- Fixes error message when archive initialization fails.
- Fixes lvcreate to remove unused cow volume if the snapshot creation fails.
- Removes old metadata backup file after renaming VG.
- Avoids scanning empty metadata areas for VG names.
- Fixes fsadm to pass --test from lvresize and prevents from checking mounted file system.
- Fixes lvresize size conversion for fsadm when block size is not 1K.
- Fixes cached volume group metadata to cope with duplicate volume group names.
- Fixes pvs segfault when pv mda attributes requested for not available PV.
- Fixes pvs segfault when run with orphan PV and some VG fields.
- Fixes lvmdump /sys listing to include virtual devices directory.
- Avoids exceeding LV size when wiping device.
- Calculates mirror log size instead of using 1 extent.
- Ensures requested device number is available before activating with it.
- Fixes incorrect exit status from 'help <command>'.
- Fixes vgrename using UUID if there are VGs with identical names.
- Fixes segfault when invalid field given in reporting commands.
- Copes with snapshot dependencies when removing a whole VG with lvremove.
- Exits with non-zero status from vgdisplay if couldn't show any requested VG.
- Fixes minimum width of devices column in reports.
- Fixes pvs report for orphan PVs when segment attributes are requested.
- Fixes pvs -a output to not read volume groups from non-PV devices.

- Fixes and updates to man pages including the restriction on file descriptors at invocation and --nameprefixes, --unquoted, --rows options in pvs,vgs,lvs commands.
- As well, this update adds the following enhancements:
- Online resizing of mirrors is now enabled.
- Adds vgimportclone command to import and rename duplicated volume group (e.g. a hardware snapshot).
- Adds --dataalignment to pvcreate to specify alignment of data area.
- Reduces memory usage by using per volume group memory pools.
- Detects and conditionally wipes swapspace signatures in pvcreate.
- Adds sparse snapshot devices manipulation, e.g. lvcreate --virtualsize (hidden zero origin).
- Inherits readahead setting from underlying devices during activation.
- Adds MMC (mmcblk) device type to filters.
- Does not scan devices if reporting only attributes from PV label.
- Adds fsadm support for reszing ext4 filesystems.
- Adds "--refresh" functionality to vgchange and vgmknodes.
- Adds lvs origin_size, dev_size, pv_mda_size and vg_mda_size to reports.

Users of lvm2 are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

1.136. lvm2-cluster

1.136.1. RHBA-2009:1394: bug-fix and enhancement update

Updated lvm2-cluster packages that fix several bugs and add enhancements are now available.

The lvm2-cluster packages contain support for Logical Volume Management (LVM) in a clustered environment.

This update ensures that the bugs fixed by the lvm2 advisory are also fixed in a clustered environment.

This update applies the following bug fixes:

- Fixes partial activation support in clustered mode.
- Flushes memory pool and fixes locking in clvmd refresh and backup command.
- Destroys toolcontext on exit in clvmd (fixes memory pool leaks).
- Fixes remote metadata backup for clvmd.
- Fixes startup race in clvmd.
- This update adds the following enhancements:
- Introduces CLVMD_CMD_LOCK_QUERY command for clvmd.
- Allows clvmd to start up if its lockspace already exists.

- Blocks SIGTERM & SIGINT in clvmd subthreads.

Users of lvm2-cluster are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

1.137. m2crypto

1.137.1. RHBA-2009:1351: bug fix update

An updated m2crypto package that fixes various bugs is now available.

The m2crypto package contains a Python module that makes it possible to call OpenSSL functions from Python scripts.

Bugs fixed in this updated package include:

- closing a file object returned by m2urllib2 did not immediately close the underlying network connection. This could cause a process to run out of file handles. Closing a file object now closes the sockets associated with it and avoids leaking file descriptors. (BZ#460692)
- the Python global interpreter lock was not released by blocking m2crypto functions, making it impossible to use m2crypto concurrently in a multi-threaded program. M2Crypto now uses the thread support in SWIG for functions that are likely to block. M2Crypto can now accept additional connections even when a different thread is still waiting for incoming data. (BZ#472690)
- m2urllib2 used absolute URIs in HTTP requests instead of using only the selector part of the URI, which is not supported by some HTTP servers. Now, m2urllib2 makes requests with only the selector part of the URI, ensuring that the request is understood even by HTTP servers that do not support requests made with the absolute URI. (BZ#491674)
- the M2Crypto SSL certificate checker incorrectly rejected certificates with a subjectAltName extension that did not contain a host name. M2Crypto now uses the certificate subject field instead of subjectAltName if subjectAltName does not contain a host name. (BZ#504060)
- the OpenSSL locking callback in M2Crypto did not block on a lock when the lock was held by another thread. This could cause data corruption in multi-threaded applications. The locking callback now functions correctly, regardless of which thread holds the lock. (BZ#507903)

Users are advised to upgrade to this updated m2crypto package, which resolves these issues.

1.138. man-pages-ja

1.138.1. RHBA-2009:0483: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0483

An updated man-pages-ja package that fixes multiple typos is now available.

The man-pages-ja package contains the manual pages from the Linux Documentation Project translated into Japanese.

This updated package addresses the following bugs:

- modules loaded after sysctl was run could override parameters set in sysctl and sysctl.conf. Man pages have been updated with information about this process and suggestions as to how modifications can be retained by the system across reboots. (BZ#451238)
- The bash(1), echo(1), wall(1), vmstat(8) and edquota(8) man pages included in the previous releast of man-pages-ja contained several typographical errors. These have now been corrected. (BZ#454048 , BZ#454419 , BZ#457361 , BZ#460688 , BZ#493783)

All man-pages-ja users should upgrade to this updated package, which resolves these issues.

1.139. mcelog

1.139.1. RHBA-2009:1374: bug fix and enhancement update

An updated mcelog package that adds support for newer Intel hardware and fixes two bugs is now available.

mcelog is a utility that allows the root user to decode machine check errors (MCE).

This update addresses the following two bugs:

- the code that generates the MCE log contained a typo that appeared in several places. Consequently, mcelog would ignore a chunk of the data at the beginning of each record. The chunk of data would be so large that each record would be empty and therefore, the log itself would be empty. With this typo corrected, mcelog correctly generates its log of MCE events. (BZ#501512)
- mcelog is unable to obtain MCE data from paravirtualized Xen guests on a system. Previously, each time that mcelog tried and failed to obtain this data, it would generate an error report -- by default, once per hour. These error reports could mislead users to think that there was a problem with their system. Now, mcelog does not generate error reports when it cannot obtain MCE data from paravirtualized Xen guests, and therefore avoids any potential confusion. (BZ#511126)

As well, this update adds the following enhancement:

- the mcelog package had not been updated in several releases. Therefore, the existing package could not decode MCE events from newer Intel processors such as the "Nehalem" and "Dunnington" series. This update adds support for newer Intel hardware. (BZ#473392)

Users are advised to upgrade to the mcelog-0.9pre-1.24 which fixes these bugs and adds support for new Intel hardware.

1.140. mdadm

1.140.1. RHBA-2009:1382: bug fix and enhancement update

An updated mdadm package that fixes several bugs and adds an enhancement is now available.

mdadm is used to create, manage, and monitor Linux MD (software RAID) devices. It provides similar functionality to the raidtools package.

This updated package fixes the following bugs:

- the Linux software raid stack supports data scrubbing (reading disks in the raid array and looking for bad sectors, and when bad sectors are found using information from other disks or from parity to rewrite the bad sectors with good data). However, the mdadm package did not make use of this functionality. This

package adds a cron job to /etc/cron.weekly to check disks for bad sectors and repair them when found. (BZ#233972)

- the mdadm man page contained several typos and was not clear on the proper usage of a number of mdadm options. The typos have been removed and notes and clarifications have been added so that the man page now better reflects the proper usage and limitations of the mdadm command. (BZ#434670 , BZ#434671 , BZ#489476)

- mdadm did not recognize the "-N" and "-Y" short options, although it recognized their long equivalents ("--name" and "--export") and they were listed as valid in mdadm --help. Mdadm now recognizes these short options. (BZ#478977)

- a new raid-check script (see the enhancement note below) attempted to check arrays that were not checkable. The script first retrieved a list of active arrays from /proc/mdstat then attempted to write "check" to the sync_action element of each array's sysfs entry. Non-redundant arrays (such as linear and raid0 arrays) do not have a sync_action entry in sysfs, however. Note: this did not prevent the script from checking arrays that could be checked but did cause cron job output errors to be e-mailed to the system administrator. The raid-check script now checks for a sync_action element in sysfs before writing to it. (BZ#513473)

This update also adds the following enhancement:

- with this update mdadm has new functionality to enable "data scrubbing" on redundant arrays. Data scrubbing looks for bad sectors on drives in redundant arrays and fixes the bad sectors using data from other drives to reconstruct sectors that return read errors. Note: data scrubbing is on by default in this new package. It runs once per week and may cause some performance degradation while it is running. If users wish to disable this feature for performance reasons, or if they wish to control what type of check is performed on arrays, or which arrays to check at all, edit the file /etc/sysconfig/raid-check. Details of how to set options are included in the file as comments. (BZ#513200)

This package also updates the upstream source base from mdadm-2.6.4 to mdadm-2.6.9. For a list of the changes and bug fixes included via this upstream update, please read the various ANNOUNCE-* files located in /usr/share/doc/mdadm-2.6.9 after installing the updated mdadm-2.6.9 package.

All mdadm users are advised to upgrade to this updated package, which resolves these issues and adds this feature.

1.141. microcode_ctl

1.141.1. RHEA-2009:1363: enhancement update

An updated module-init-tools package that adds an enhancement is now available.

microcode_ctl is a kernel-related package that provides utility code and the microcode data itself - supplied by Intel - to assist the kernel in updating the CPU microcode at system boot time.

This updated microcode_ctl includes the latest 20090330 version of the Intel-supplied microcode data. This microcode corrects the behavior of various Intel processors, as described in processor specification updates issued by Intel for those processors. (BZ#463445)

Users are advised to upgrade to this updated microcode_ctl package, which adds this enhancements.

1.142. mkinitrd

1.142.1. RHBA-2009:1088: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1088

Updated mkinitrd packages that resolve an issue are now available.

The mkinitrd utility creates file system images for use as initial ramdisk (initrd) images.

These updated mkinitrd packages fix the following bug:

- when using kernel version 2.6.18-122 or earlier, creating an initial ramdisk (initrd) failed due to the mkinitrd script assuming that RAID-specific kernel modules were available when they were not. With these updated packages, mkinitrd no longer assumes that these RAID-specific kernel modules are available, and thus initrd creation completes successfully. (BZ#496591)

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

1.142.2. RHBA-2009:1345: bug fix and enhancement update

Updated mkinitrd packages that fix several bugs and add enhancements are now available.

The mkinitrd utility creates file system images for use as initial ramdisk (initrd) images.

This update includes fixes for the following bugs:

- mkinitrd failed on dmraid systems with kernels that don't include dm-raid45 modules. (BZ479270)
- the "netname" command has been improved to handle environmental variables correctly. (BZ474422)
- handling for UUID and LABEL on hibernation devices has been improved. (BZ489836)
- This update also includes these enhancements:
- when in fips mode the tcrypt module is now loaded to self-test all cryptographic algorithms. (BZ499639)
- support for FIPS integrity checking of the kernel has been added. (BZ467497)

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

1.143. mlocate

1.143.1. RHBA-2009:1251: bug fix update

An updated mlocate package that disables scanning GFS file systems by default is now available.

mlocate is a locate/updatedb implementation. It keeps a database of all existing files and allows you to lookup files by name.

The updatedb program is configured by the mlocate package to run daily. In its default configuration, updatedb scans included GFS and GFS2 file systems. Running updatedb concurrently on multiple nodes leads to lock contention and large changes in cache usage. This substantially reduces the effective performance of the file system. This update excludes GFS volumes from the updatedb scan by default. As a consequence, locate(1) will not report files located on GFS volumes. (BZ#221547)

Users are advised to upgrade to this updated mlocate package.

1.144. mod_auth_mysql

1.144.1. RHSA-2009:0259: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0259

An updated mod_auth_mysql package to correct a security issue is now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The mod_auth_mysql package includes an extension module for the Apache HTTP Server which can be used to implement web user authentication against a MySQL database.

A flaw was found in the way mod_auth_mysql escaped certain multibyte-encoded strings. If mod_auth_mysql was configured to use a multibyte character set that allowed a backslash '\' as part of the character encodings, a remote attacker could inject arbitrary SQL commands into a login request. (CVE-2008-2384)

Note: This flaw only affected non-default installations where AuthMySQLCharacterSet is configured to use one of the affected multibyte character sets. Installations that did not use the AuthMySQLCharacterSet configuration option were not vulnerable to this flaw.

All mod_auth_mysql users are advised to upgrade to the updated package, which contains a backported patch to resolve this issue. After installing the update, the httpd daemon must be restarted for the fix to take effect.

1.145. mod_authz_ldap

1.145.1. RHBA-2009:0305: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0305

An updated mod_authz_ldap package that fixes a bug is now available.

mod_authz_ldap is a module for the Apache HTTP Server which provides support for authenticating users against an LDAP database.

This updated mod_authz_ldap package fixes a bug which resulted in random data being logged to the access_log instead of the appropriate string when the "AuthzLDAPSetAuthorization" directive was used.

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

1.146. mod_nss

1.146.1. RHEA-2009:0403: enhancement update

Note

This update has already been released (prior to the GA of this release) as errata RHEA-2009:0403

An enhanced mod_nss package is now available.

mod_nss provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

This update back-ports the PassphraseDialog "defer" configuration option in NSS. When this parameter is set to "defer", only those tokens listed in the file are authenticated at startup. With the "builtin" and "file" options for the PassphraseDialog parameter, all tokens are authenticated, even if the token password is not defined. That can cause an authentication failure which prevents the Apache server from starting.

1.146.2. RHBA-2009:1365: bug fix update

An update mod_nss package that fixes a bug in proxy handling is now available.

mod_nss provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

This update addresses a proxy handling bug in mod_nss. mod_nss was not handling blocked reads properly. Rather than attempting the read again, it failed with an "End of File" message. When used with mod_proxy in a reverse proxy configuration, this would sometimes result in returning only part of the remote content. (Bugzilla #484380)

mod_proxy has a single API for SSL handling, and mod_nss doesn't register to handle SSL proxy requests if mod_ssl is loaded. In order for mod_nss to work with mod_proxy, mod_ssl must be removed or disabled. It can be disabled in one of two ways:

- By removing the mod_ssl package
- By removing or renaming /etc/httpd/conf.d/ssl.conf

Apache users requiring SSL and TLS cryptography are advised to install this updated package.

1.147. module-init-tools

1.147.1. RHBA-2009:1362: bug fix update

Updated module-init-tools packages that address several bugs are now available.

module-init-tools is a kernel-related package that provides utilities for automatically loading and unloading drivers, as well as finding out about drivers that are installed on a given Red Hat Enterprise Linux system.

These updated packages fix the following issues:

- this updated module-init-tools package provides an enhancement that enables module parameters to be read automatically from the kernel command line in the same fashion that built-in kernel modules are handled.(BZ#487395)
- previously, in some cases, a kernel module package may have installed an older version of an already-installed kernel module. When this occurred, the manner in which the kernel modules were sorted may

have resulted in an older version of the module being enabled by default. While the installation of multiple versions of the same kernel module on a system is unsupported, this update provides provides improvements to the sorting of kernel modules so that the highest version is used, which resolves this issue. (BZ#404311)

- previously, the "weak-modules --add-modules" command created a redundant directory structure in the "weak-updates/" directory. With this update, the "--add-modules" option now creates the same structure as the "weak-modules --add-kernels" command. (BZ#484762)
- previously, the "modprobe --show-depends" command returned "install" command directives, causing issues with some kernel modules. With this update, the "--show-depends" correctly outputs the "insmod" records, which resolves this issue. (BZ#497923)
- previously, the man page for depmod (a tool used to generate a list of kernel module dependencies) was missing documentation for the "-a" option. In this updated package, the depmod man page has been amended with the following description of the "-a" option:

```
-a --all
  Probe all modules. This option is enabled by default if no file names
  are given in the command-line.
```

(BZ#475549)

Users are advised to upgrade to these updated module-init-tools packages, which resolve these issues.

1.148. mysql

1.148.1. RHSA-2009:1289: Moderate security and bug fix update

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

MySQL did not correctly check directories used as arguments for the DATA DIRECTORY and INDEX DIRECTORY directives. Using this flaw, an authenticated attacker could elevate their access privileges to tables created by other database users. Note: This attack does not work on existing tables. An attacker can only elevate their access to another user's tables as the tables are created. As well, the names of these created tables need to be predicted correctly for this attack to succeed. (CVE-2008-2079)

A flaw was found in the way MySQL handles an empty bit-string literal. A remote, authenticated attacker could crash the MySQL server daemon (mysqld) if they used an empty bit-string literal in an SQL statement. This issue only caused a temporary denial of service, as the MySQL daemon was automatically restarted after the crash. (CVE-2008-3963)

An insufficient HTML entities quoting flaw was found in the mysql command line client's HTML output mode. If an attacker was able to inject arbitrary HTML tags into data stored in a MySQL database, which was later retrieved using the mysql command line client and its HTML output mode, they could perform a cross-site scripting (XSS) attack against victims viewing the HTML output in a web browser. (CVE-2008-4456)

Multiple format string flaws were found in the way the MySQL server logs user commands when creating and deleting databases. A remote, authenticated attacker with permissions to CREATE and DROP databases could use these flaws to formulate a specifically-crafted SQL command that would cause a temporary denial of service (open connections to mysqld are terminated). (CVE-2009-2446)

Note

To exploit the CVE-2009-2446 flaws, the general query log (the mysqld "--log" command line option or the "log" option in "/etc/my.cnf") must be enabled. This logging is not enabled by default.

This update also fixes multiple bugs:

- an error in the mysqld init script caused the MySQL service to not wait correctly if the socket file specified in /etc/my.cnf was anything other than the default. This caused MySQL to return an erroneous "[FAILED]" message. With this update, /etc/init.d/mysqld has been corrected, MySQL waits correctly and the erroneous error message no longer presents. (BZ#435494)

- when slave DBs rotated relay logs, the file was deleted and the relay log index file was then edited. If the slave shut down before the index file was edited, said file contained a reference to a now non-existent relay log. In some circumstances, this could cause a race condition or a replication failure when restarting slave DB. With this update, the relay log index file is updated before the relay log file is deleted, ensuring the race condition or replication failure can not occur. (BZ#448534)

- the mysqld init script did not check that mysql ran as the mysql user. It also did not explicitly initialize the MySQL database in the directory specified in my.conf. With this update, both these oversights have been rectified. Note: the absence of these checks did not prevent a default MySQL installation initializing successfully. (BZ#450178)

- in one reported instance, upgrading from MySQL 5.0.22 to MySQL 5.0.45 caused a large database to repeatedly crash on launch. The crashes ceased when MySQL was further upgraded to version 5.0.51b. This updated package upgrades MySQL to version 5.0.77, which incorporates the changes made in 5.0.51b. (BZ#452824)

- as of MySQL 5.0.42, DATE values are compared as ints not strings. Consequent to this, using DATE() in a WHERE clause did not return any records after a NULL value. The null_value flag was not reset, causing all values following the first NULL value encountered to also be treated as NULL. With this update, the flag is reset correctly and the DATE() function returns records as expected. (BZ#453156)

- the tmpdir variable was not honored for temporary tables created for filesorts. .frm files were created correctly but data files were written to the working directory. Depending on the working directory's location, MySQL could slow to a crawl or even appear to hang. With this update, the tmpdir variable is honored as expected. (BZ#455619)

- for large enough query caches, invalidating a data subset took too long, effectively freezing the server. Dictionary access requests are now limited to 0.1 seconds. For longer requests, the system falls back to ordinary statement execution. Note: this does not work for query cache invalidations issued by DROP, ALTER or RENAME TABLE operations. (BZ#456875)

- in a stored function or trigger, when InnoDB detected a deadlock it attempted a rollback and displayed an incorrect ERROR 1422 message. In practice this meant, if two concurrent transactions updated the same table, the second would display the erroneous error. InnoDB now returns an error under these conditions and does not attempt a rollback. (BZ#457218)

- equivalent paths in MySQL config files (eg, ~/.my.cnf and SYSCONFDIR/my.cnf), could be read twice at startup. SYSCONFDIR/my.cnf was also read last, so ~/.my.cnf did not override as expected. Paths are now normalized and duplicates removed before the list is read; also, SYSCONDIR/my.cnf is now read before ~/.my.cnf. (BZ#462534)

- when MyISAM keys were fetched, a key block pointer was copied to the end of the key buffer but the pointer length was not accounted for when the buffer size was calculated. This could cause memory overwrites which, in turn, lead to unpredictable results. Given this unpredictability there is no simple test case. One known consequence, however, is queries that, in some cases, produced a result set using

ORDER BY ASC but returned no results when using ORDER BY DESC. With this update, the key buffer size has been increased by the length of the key block pointer. Memory overwrites no longer occur and, consequently, queries return results as expected when ORDER BY DESC is used. (BZ#470036)

- when a client connection exited without calling mysql_close(), the aborted_threads variable was updated twice and the aborted_clients status variable was consequently incremented twice. With this update, aborted_threads is updated in only one place, preventing the second, erroneous, aborted_clients incrementation. (BZ#479615)

Note: Some further upstream fixes are documented in the MySQL 5.0.77 Release Notes

All MySQL users are advised to upgrade to these updated packages, which resolve these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

1.149. mysql-connector-odbc

1.149.1. RHBA-2009:1290: bug fix update

An updated mysql-connector-odbc package that fixes several bugs is now available.

mysql-connector-odbc is an ODBC (rev 3) driver for MySQL, for use with unixODBC.

With this update, mysql-connector-odbc has been updated from version 3.51.12 to version 3.51.26. This new version incorporates several upstream bug fixes. Details regarding these fixes can be found in the Changes in MYSQL Connector/ODBC file, linked to in the References section below.

In particular, this update fixes an error where SQLDriverConnect threw an unexpected 'setup cannot be opened' exception. (BZ#460293)

MySQL and ODBC users should upgrade to this updated package, which resolves this and other issues.

1.150. nautilus-sendto

1.150.1. RHBA-2008:0916: bug fix and enhancement update

An updated nautilus-sendto package that fixes several bugs and adds enhancements is now available.

The nautilus-sendto package provides a Nautilus context menu for sending files via other desktop applications. These functions are implemented as plugins, so nautilus-sendto can be extended with additional features.

This update addresses the following issue:

- when nautilus-sendto was enabled for Pidgin, the contextual menu in Nautilus referred to 'Gaim' rather than 'Pidgin'. With this update, the menu item text has been corrected and the contextual menu refers to Pidgin as expected. (BZ#250403)

This updated package also rebases nautilus-sendto from version 0.7 to upstream version 1.0.1:

- this rebase adds the ability to send to Bluetooth devices, provides better Pidgin integration, and makes a number of user interface fixes. See the ChangeLog, installed to /usr/share/doc/nautilus-sendto-1.0.1/ for details regarding these and other changes. (BZ#250403)

All Nautilus-sendto users are advised to upgrade to this updated package, which resolves these issues and adds these enhancements.

1.151. net-snmp

1.151.1. RHBA-2009:1215: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1215

Updated net-snmp packages that resolve an issue are now available.

The Simple Network Management Protocol (SNMP) is a protocol used for network management. The net-snmp packages include 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, a version of the netstat command which uses SNMP, and a Tk/Perl MIB browser.

These updated net-snmp packages fix the following bug:

- snmpd, the SNMP daemon, did not expect the packet counters in the /proc/net/snmp and /proc/net/snmp6 files to be 64-bit on 64-bit systems. When these counters exceeded 32 bits in size, which would occur when the Linux kernel sent or received greater than 4,294,967,296 (2^32) packets, then the snmpd daemon would terminate abnormally. With this update, the snmpd daemon no longer crashes when it encounters a packet counter in the directories listed above that is greater than 32 bits in size, thus resolving the issue. (BZ#516182)

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

1.151.2. RHBA-2009:1069: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1069

Updated net-snmp packages that resolve an issue are now available.

The Simple Network Management Protocol (SNMP) is a protocol used for network management. The net-snmp packages include 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, a version of the netstat command which uses SNMP, and a Tk/Perl MIB browser.

These updated net-snmp packages fix the following bug:

- snmpd, the SNMP daemon, contained several memory leaks. These leaks caused snmpd to leak memory relatively slowly but significantly, at the rate of 50 MB per month. These memory leaks have been plugged in these updated packages, and snmpd no longer leaks memory over time. (BZ#497810)

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

1.151.3. RHBA-2009:1372: enhancement and bug fix update

Updated net-snmp packages that fix various bugs and add enhancements are now available.

The Simple Network Management Protocol (SNMP) is a protocol used for network management. The net-

snmp packages include 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; a version of the netstat command which uses SNMP; and a Tk/Perl MIB browser.

These updated net-snmp packages provide fixes for the following bugs:

- using "snmpwalk" to walk a host with automounted NFS mounts sometimes resulted in the snmpd server timing out if the NFS mount became unresponsive. This update provides a new directive for the snmpd.conf configuration file, "skipNFSInHostResources", which allows snmpwalk to skip over automounted NFS mounts when performing a walk. (BZ#461631)
- the snmp daemon did not correctly report the speeds of network interfaces when they were greater than 4 Gbit/s. With this update, the actual speed of 10-Gigabit Ethernet (10GbE) network cards are accurately reported. (BZ#464061)
- the snmpd daemon no longer prints spurious "error on subcontainer " insert (-1)" messages to snmpd.log when it reloads its configuration file (such as when the daemon is restarted). (BZ#468147)
- the snmpd daemon no longer reports the following errors to syslog when walking through diskIOTable: "diskio.c: don't know how to handle [x] request". (BZ#474093)
- the net-snmp packages were upgraded to upstream version 5.3.2.2 for Red Hat Enterprise Linux 5.3. This update changed the format for the snmpd daemon's "-LS [level] [facility]" logging options by removing the required space from between the [level] and [facility] arguments. These updated packages now support both the old-style "-LS" option formatting (space between arguments) and the new-style (space-less) formatting. (BZ#477768)
- the snmpd daemon contained several memory leaks which occurred when accessing the Stream Control Transmission Protocol Management Information Base (SCTP-MIB). These memory leaks have been fixed with these updated packages. (BZ#497280)
- the net-snmp-devel package contained an undeclared dependency on the lm_sensors-devel package, which has been made explicit with this update. (BZ#437819)

In addition, the following new Object IDs (OIDs) have been implemented in the snmpd daemon:

- RMON-MIB::etherStatsJabbers and ETHERLIKE-MIB:dot3StatsTable. The implementation of these OIDs is limited to systems with a Broadcom BCM 5708 Gigabit Ethernet Controller or an Intel Corporation 82541GI Gigabit Ethernet Controller. (BZ#468832)
- IP-MIB::ipAddressSpinLock, which allows the synchronization of ipTable modifications. (BZ#479609)
- IP-MIB::ipNetToPhysicalLastUpdated, which details when a ipNetToPhysicalTable was created or last updated. (BZ#477092)

All SNMP users are advised to upgrade to these updated net-snmp packages, which resolve these issues and add these enhancements.

1.152. netpbm

1.152.1. RHSA-2009:0012: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0012

Updated netpbm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The netpbm package contains a library of functions for editing and converting between various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps), and others.

An input validation flaw and multiple integer overflows were discovered in the JasPer library providing support for JPEG-2000 image format and used in the jpeg2ktopam and pamtojpeg2k converters. An attacker could create a carefully-crafted JPEG file which could cause jpeg2ktopam to crash or, possibly, execute arbitrary code as the user running jpeg2ktopam. (CVE-2007-2721, CVE-2008-3520)

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

1.152.2. RHBA-2009:1268: bug fix update

Updated netpbm packages that resolve several issues and provide enhancements are now available.

The netpbm package contains a library of functions which support programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps) and others.

These updated netpbm packages upgrade netpbm to version 10.35.58, which provides many bug fixes and enhancements over the previous version. Notably, a few new utilities are included in this upgraded version, including: jbigtopnm, pcdovtoppm and pnmtojbig.

In addition, the following bugs have been fixed in this netpbm update:

- several utilities shipped with netpbm may have crashed while processing image files. With this update, this issue has been resolved.
- several utilities shipped with netpbm did not accept files from standard input even though this method was in accordance with the documentation. With this update, this issue has been resolved.
- the documentation of a number of utilities provided by netpbm did not agree with the actual usage, described parameters which are not present, and contained various typos and errors. The documentation of the netpbm utilities is much improved with this update, and the specific problems listed have been corrected.

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

1.153. nfs-utils

1.153.1. RHSA-2009:1321: Low security and bug fix update

An updated nfs-utils package that fixes a security issue and several bugs is now available.

This update has been rated as having low security impact by the Red Hat Security Response Team.

The nfs-utils package provides a daemon for the kernel NFS server and related tools.

It was discovered that nfs-utils did not use tcp_wrappers correctly. Certain hosts access rules defined in "/etc/hosts.allow" and "/etc/hosts.deny" may not have been honored, possibly allowing remote attackers to bypass intended access restrictions. (CVE-2008-4552)

This updated package also fixes the following bugs:

- the "LOCKD_TCPPORT" and "LOCKD_UDPPORT" options in "/etc/sysconfig/nfs" were not honored: the lockd daemon continued to use random ports. With this update, these options are honored. (BZ#434795)
- it was not possible to mount NFS file systems from a system that has the "/etc/" directory mounted on a read-only file system (this could occur on systems with an NFS-mounted root file system). With this update, it is possible to mount NFS file systems from a system that has "/etc/" mounted on a read-only file system. (BZ#450646)
- arguments specified by "STATDARG=" in "/etc/sysconfig/nfs" were removed by the nfslock init script, meaning the arguments specified were never passed to rpc.statd. With this update, the nfslock init script no longer removes these arguments. (BZ#459591)
- when mounting an NFS file system from a host not specified in the NFS server's "/etc/exports" file, a misleading "unknown host" error was logged on the server (the hostname lookup did not fail). With this update, a clearer error message is provided for these situations. (BZ#463578)
- the nhfsstone benchmark utility did not work with NFS version 3 and 4. This update adds support to nhfsstone for NFS version 3 and 4. The new nhfsstone "-2", "-3", and "-4" options are used to select an NFS version (similar to nfsstat(8)). (BZ#465933)
- the exportfs(8) manual page contained a spelling mistake, "djando", in the EXAMPLES section. (BZ#474848)
- in some situations the NFS server incorrectly refused mounts to hosts that had a host alias in a NIS netgroup. (BZ#478952)
- in some situations the NFS client used its cache, rather than using the latest version of a file or directory from a given export. This update adds a new mount option, "lookupcache=", which allows the NFS client to control how it caches files and directories. Note: The Red Hat Enterprise Linux 5.4 kernel update (the fourth regular update) must be installed in order to use the "lookupcache=" option. Also, "lookupcache=" is currently only available for NFS version 3. Support for NFS version 4 may be introduced in future Red Hat Enterprise Linux 5 updates. Refer to Red Hat Bugzilla #511312 for further information. (BZ#489335)

Users of nfs-utils should upgrade to this updated package, which contains backported patches to correct these issues. After installing this update, the nfs service will be restarted automatically.

1.154. nfs-utils-lib

1.154.1. RHBA-2009:1250: bug fix update

Updated nfs-utils-lib packages that fix a bug are now available.

The nfs-utils-lib package contains support libraries required by programs in the nfs-utils package.

These updated packages apply a fix for the following bug:

- when resolving a group ID, a group's data structure is stored in a buffer. When the buffer size was exceeded, the default no-group value was used in place of the group ID, removing certain user privileges. Larger buffer spaces are now provided when the defined buffer is exceeded, so groups are mapped to the appropriate ID. (BZ#453804)

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

1.155. nfs4-acl-tools

1.155.1. RHEA-2009:1407: enhancement update

Updated nfs4-acl-tools packages that fix a bug are now available.

The nfs4-acl-tools packages provide utilities for managing NFSv4 Access Control Lists (ACLs) on files and directories mounted on ACL-enabled NFSv4 file systems. These updated packages fix the following bug:

- the mapping between ACLs in the draft POSIX standard and NFSv4 ACLs used in previous versions of the nfs4-acl-tools did not accept all NFSv4 ACLs. As a result, attempts to set an ACL on an NFS server could fail with the message "Operation not supported". Nfs4-acl-tools has been rebased to upstream version 0.3.3, which contains completely new mapping code that handles practically all NFSv4 ACLs. (BZ#507443)

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

1.156. nspr and nss

1.156.1. RHSA-2009:1186: Critical security, bug fix, and enhancement update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1186

Updated nspr and nss packages that fix security issues, bugs, and add an enhancement are now available for Red Hat Enterprise Linux 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The packages with this update are identical to the packages released by RHBA-2009:1161 on the 20th of July 2009. They are being reissued as a Red Hat Security Advisory as they fixed a number of security issues that were made public today. If you are installing these packages for the first time, they also provide a number of bug fixes and add an enhancement, as detailed in RHBA-2009:1161. Since the packages are identical, there is no need to install this update if RHBA-2009:1161 has already been installed.

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.

These updated packages upgrade NSS from the previous version, 3.12.2, to a prerelease of version 3.12.4. The version of NSPR has also been upgraded from 4.7.3 to 4.7.4.

Moxie Marlinspike reported a heap overflow flaw in a regular expression parser in the NSS library used by browsers such as Mozilla Firefox to match common names in certificates. A malicious website could present a carefully-crafted certificate in such a way as to trigger the heap overflow, leading to a crash or, possibly, arbitrary code execution with the permissions of the user running the browser. (CVE-2009-2404)

Note: in order to exploit this issue without further user interaction in Firefox, the carefully-crafted certificate would need to be signed by a Certificate Authority trusted by Firefox, otherwise Firefox presents the victim with a warning that the certificate is untrusted. Only if the user then accepts the certificate will the overflow take place.

Dan Kaminsky discovered flaws in the way browsers such as Firefox handle NULL characters in a certificate. If an attacker is able to get a carefully-crafted certificate signed by a Certificate Authority trusted by Firefox, the attacker could use the certificate during a man-in-the-middle attack and potentially confuse Firefox into accepting it by mistake. (CVE-2009-2408)

Dan Kaminsky found that browsers still accept certificates with MD2 hash signatures, even though MD2 is no longer considered a cryptographically strong algorithm. This could make it easier for an attacker to create a malicious certificate that would be treated as trusted by a browser. NSS now disables the use of MD2 and MD4 algorithms inside signatures by default. (CVE-2009-2409)

All users of nspr and nss are advised to upgrade to these updated packages, which resolve these issues and add an enhancement.

1.156.2. RHBA-2009:1161: bug fix and enhancement update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1161

Updated nspr and nss packages that fix several bugs and add an enhancement are now available

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.

These updated packages upgrade nss from the previous version, 3.12.2, to a prerelease of version 3.12.4. The version of nspr has also been upgraded, from 4.7.3 to 4.7.4. These version upgrades provide fixes for the following bugs:

SSL client authentication failed against an Apache server when it was using the mod_nss module and configured for NSSOCSP.

On the client side, the user agent received an error message that referenced "Error Code: -12271" and stated that establishing an encrypted connection had failed because the certificate had been rejected by the host.

On the server side, the nss_error_log under /var/log/httpd/ contained the following message: "[error] Re-negotiation handshake failed: Not accepted by client!?"

Also, /var/log/httpd/error_log contained this error message: "SSL Library Error: -8071 The OCSP server experienced an internal error."

With these updated packages, the dependency problem which caused this failure has been resolved so that SSL client authentication with an Apache web server using mod_nss which is configured for NSSOCSP succeeds as expected. Note that if the presented client certificate is expired, then access is denied, the user agent is presented with an error message about the invalid certificate, and the OCSP queries are seen in the OCSP responder. Also, similar OCSP status verification happens for SSL server certificates used in Apache upon instance start or restart. (BZ#499052)

Attempting client authorization with a certificate authority when using ECC (Elliptic Curve Cryptography) on a machine with a hardware security module (HSM) failed with an error message stating that the browser (the test agent in this case) was unable to authenticate to the agent URL. This has been fixed in these updated packages so that agents are once again able to authenticate with certificate authorities when using the ECC algorithm on machines with an HSM. (BZ#223279)

In addition, these updated packages provide an enhancement to update cryptography services required by the Openswan package. (BZ#502201)

All users of nspr and nss are advised to upgrade to these updated packages, which resolve these issues and provide these enhancements.

1.157. nss_ldap

1.157.1. RHBA-2009:1379: bug fix update

An updated nss_ldap package is now available for Red Hat Enterprise Linux 5.

The nss_ldap module is a plugin for the standard C library which allows applications to look up information about users and groups using a directory server.

This updated nss_ldap package provide fixes for the following bugs:

- nss_ldap contained a socket descriptor leak that occurred when it was forced to reconnect to the LDAP server. This socket descriptor leak would eventually cause the nscd daemon to consume 100% CPU and fail to reconnect to the LDAP server. This has been fixed so that sockets do not leak and a failure to reconnect does not occur. (BZ#428837)
- this update modifies the nss_ldap module's behavior so that when it encounters an entry which contains an attribute value which is expected to be numeric, but the value contained in the entry can not be correctly parsed as a number, then the module ignores the entry. (BZ#457258)
- a previous change in nss_ldap's default behavior meant that the "getent passwd" command retrieved a fewer number of lines than before. This default behavior can be changed with the "nss_paged_results" option, which, in these updated packages, is now set by default to "no", so that "getent passwd" is able to retrieve up to 40447 lines instead of 1041. (BZ#486321)
- running the command "id [ldap_username]" when the "nss_connect_policy" directive in the /etc/ldap.conf configuration file was set to "oneshot" caused the "id" command to fail and the nscd daemon to crash due to an assertion failure. With these updated packages, calling "id [user_name]" when "nss_connect_policy" is set to "oneshot" works as expected and no longer triggers the failed assertion. (BZ#488857)

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

1.158. ntp

1.158.1. RHSA-2009:1039: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1039

An updated ntp package that fixes two security issues is now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Network Time Protocol (NTP) is used to synchronize a computer's time with a referenced time source.

A buffer overflow flaw was discovered in the ntpd daemon's NTPv4 authentication code. If ntpd was configured to use public key cryptography for NTP packet authentication, a remote attacker could use this flaw to send a specially-crafted request packet that could crash ntpd. (CVE-2009-1252)

Note

NTP authentication is not enabled by default.

A buffer overflow flaw was found in the ntpq diagnostic command. A malicious, remote server could send a specially-crafted reply to an ntpq request that could crash ntpq. (CVE-2009-0159)

All ntp users are advised to upgrade to this updated package, which contains backported patches to resolve these issues. After installing the update, the ntpd daemon will be restarted automatically.

1.158.2. RHSA-2009:0046: Moderate security update

Important

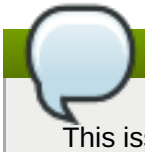
This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0046

Updated ntp packages to correct a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Network Time Protocol (NTP) is used to synchronize a computer's time with a referenced time source.

A flaw was discovered in the way the ntpd daemon checked the return value of the OpenSSL EVP_VerifyFinal function. On systems using NTPv4 authentication, this could lead to an incorrect verification of cryptographic signatures, allowing time-spoofing attacks. (CVE-2009-0021)



Note

This issue only affects systems that have enabled NTP authentication. By default, NTP authentication is not enabled.

All ntp users are advised to upgrade to the updated packages, which contain a backported patch to resolve this issue. After installing the update, the ntpd daemon will restart automatically.

1.159. numactl

1.159.1. RHBA-2009:0389: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0389

An updated numactl package that fixes a bug is now available.

numactl is Simple NUMA policy support. It consists of a numactl program to run other programs with a specific NUMA policy and a libnuma to do allocations with NUMA policy in applications.

- the numactl-devel subpackage did not require the same version as the primary numactl package. The absence of this requirement could lead to situations where the version of the primary package installed on a system differed from the version of the subpackage. In this updated package, the subpackage requires the same version of the primary package. With the version of the subpackage aligned to that of the primary package, the interoperability of these components is ensured. (BZ#467022)

Users are advised to upgrade to this updated numactl package which resolves this issue.

1.160. openais

1.160.1. RHBA-2009:1191: bug-fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1191

Updated openais packages that fix a bug are now available.

The openais packages provide the core infrastructure used by Red Hat Cluster Suite and GFS.

This update fixes the following bug:

- When a node is sending heavy transmissions, and it is killed and restarted, it can sometimes lead to complete cluster failure by not allowing new communication to occur from that node. This is a regression in the z stream.

1.160.2. RHBA-2009:1104: bug-fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1104

Updated openais packages that fix various bugs are now available.

The openais packages provide the core infrastructure used by Red Hat Cluster Suite and GFS.

This update fixes the following bugs:

- The CFG library, which is used to enable redundant ring, does not function properly.
- The CPG service, which is used throughout the cluster software, can sometimes segfault under certain loads.
- On ppc architectures, the IPC system can segfault because of how va_args and unions operate on these platforms.
- The totempg subsystem in openais can sometimes throw away a message, which can result in cluster failure.
- The IPC system contains a problem with the CPG service. The problem causes the wrong error code to be returned when the library user has insufficient permissions (regression).
- A race condition can cause the CPG service to have unexpected behavior (regression).
- Configuration changes in the CPG service could be delivered out of order (regression).

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

1.160.3. RHBA-2009:0417: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0417

Updated openais packages that fix several bugs are now available.

These packages contain the openais executive, openais service handlers, default configuration files, and init script.

This update applies the following bug fixes:

- Fix defect that results in aisexec core dumping under IPC load.
- Fix defect where cpg flow control doesn't work properly.
- Fix defect where, in many cases, certain message types can be ignored in the ckpt or cpg services.
- Fix defect where openais segfaults during addition of node and message sizes greater then the MTU.
- Fix problem with the way totem queue length is determined, which was resulting in assertions under certain heavy load conditions.
- Fix rolling upgrade problem where rolling upgrades don't work from 5.2 to 5.3.
- Fix defect where checkpoint reference counts were incorrectly calculated from a departing node in some conditions.

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

1.160.4. RHBA-2009:1366: bug-fix and enhancement update

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

The openais packages provide the core infrastructure used by Red Hat Cluster Suite and GFS.

This update fixes the following bugs:

- The CPG service, which is used throughout the cluster software, sometimes segfaulted under certain loads. (BZ#261381)
- On PowerPC architectures, the IPC system could segfault because of how va_args and unions operate on these platforms. (BZ#499767)
- The totempg subsystem in openais could sometimes throw away a message, which could result in cluster failure. (BZ#497419)
- The IPC system contained a regression with the CPG service, which caused the wrong error code to be returned when the library user has insufficient permissions. (BZ#494347)
- The redundant ring feature cannot be re-enabled after a failure, because of defects in libcfg. (BZ#494035)
- The CPG service failed to synchronize properly with nodeids greater then 0xffffff. This resulted in CPG not working when automatic node id generation was used. (BZ#489451)
- Certain message types were ignored, resulting in improper synchronization. (BZ#480684)
- The checkpoint service incorrectly calculated reference counts on checkpoints opened by an exiting node, resulting in checkpoint leak. (BZ#490099)
- Under heavy ipc connection/disconnection in the cpg service, the cpg service would segfault. (BZ#497420).
- The cpg service would segfault when cpg_join and cpg_leave were issued by multiple nodes on the same cpg group name as a result of race condition. (BZ#501561)
- The totem free queue was calculated improperly resulting in aborts under heavy cpg load. (BZ#488095)
- Under certain conditions, a race condition resulted in a double list delete in the cpg service causing segfault. (BZ#491459)
- A regression in the openais build process resulted in cmirror regressions. (BZ#496985)
- A regression in the CPG service where a race condition would occur in the delivery of configuration changes with 3+ nodes. (BZ#490098)
- A regression in the CPG service where nodes would see out-of-order configuration changes after a node was started with existing CPG groups. (BZ#504195)
- A regression in the confdb service where the shared object elf header was not properly set. (BZ#504832)
- A regression where semaphores and shared memory was leaked if service cman stop was executed. (BZ#506778)
- A regression, if aisexec was killed while transmitting, and later restarted, the cluster returned ERR_TRY_AGAIN on all API calls. (BZ#506119)

This update adds the following enhancements:

- Feature to allow rolling upgrades of the crypto stack. (BZ#497480)
- Feature to set broadcast mode instead of using multicast. (BZ#492808)

- Feature to allow uidgid files to be placed on the system to allow configurable ipc security of third party applications. (BZ#501337)

Users should upgrade to these updated packages, which resolve these issues and add these enhancements.

1.161. openhpi

1.161.1. RHEA-2009:1279: enhancement update

A new version of openhpi that updates the package to version 2.14.0 is now available.

OpenHPI is an open source project created with the intent of providing an implementation of the SA Forum's Hardware Platform Interface (HPI). HPI provides an abstracted interface to managing computer hardware, typically for chassis and rack-based servers.

The updated packages include the newest version of OpenHPI, 2.14.0. OpenHPI 2.14.0 includes multiple features and enhancements added since OpenHPI 2.10.2.

This rebase includes many bug fixes and enhancements, including:

- Addition of HP BladeSystem c-Class plug-in
- HP c-Class plugin: additional sensors.
- HP c-class-Enhancement to add IO and Storage blade support.
- HP c-Class plugin: add underpinnings for additional management functions.
- Add entries for HP c-Class plugin pdf documents in Makefile.am.
- Make use of common SSL code HP c-Class Plugin.(BZ#474176)
- Important enhancements and many bug fixes to the HP c-Class plugin
- Many bug fixes to the HPI Shell.
- HPI Shell: Severity fix for announcements added to annunciators.
- HPI Shell: fix closing session and data display.
- Added hpi_shell command to obtain version information
- Enhancements to hpi_shell including a command to reopen a session and to show a single inventory area (thanks to avpak).
- All HPI clients now report proper OpenHPI and SAF HPI version numbers to aid debugging of problems.
- OpenHPI Daemon: Hysteresis values are now validated correctly.
- Allows you to connect to multiple daemons from one client
- Obscure bug fixed in the daemon - affected IPMI plugin when it didn't find shelf manager initially
- Add Dimis and Fumis to Simulator plugin.
- Fix invalid handling of ATCA Led Controls in Manual Mode, IPMI Direct plugin.
- RTAS plugin build fixes
- Cross compilation build improvement regarding the number size checks.

- Creates separate SSL support library for future modularity among plug-ins
- Added SSL library initialization to HPI initialization
- Fixed persisted DAT issue - blank alarms
- HPI-B.03.01 support.
- A new iLO2 RIBCL plug-in for managing HP ProLiant Rack Mount servers.
- Fix domain ID reporting in redundant domains with multiple daemon connections.
- Fix installation of openhpid initscript.
- Enable redundant domains with multiple daemon connections.
- Add saHpiEventLogCapabilitiesGet to simulate plug-in.
- Support change in the OA switchover behaviour.
- Add man pages for sample openhpi applications.
- Add documentation for new ilo2_ribcl and oa_soap plug-ins HP ProLiant plug-in
- Numerous other bug fixes.

For details of these and other changes see the changelogs versions 2.11.0 through to 2.14.0, for which there are links in the References section below.

All users of the openhpi package are encouraged to upgrade to the latest version, which offers these enhancements.

1.162. openib

1.162.1. RHBA-2009:1304: bug fix update

Updated OpenFabrics Alliance packages that re-base the OFED stack and fix various bugs are now available.

The OpenFabrics Alliance Enterprise Distribution (OFED) is a collection of Infiniband and iWARP utilities, libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology. Red Hat Enterprise Linux uses the OFED software stack as its complete stack for Infiniband/iWARP/RDMA hardware support.

These updated packages re-base the OFED stack to version 1.4.1 (BZ#459652). For details regarding the changes since version 1.3.2-pre (the version previously included with Red Hat Enterprise Linux 5) see the various Release Notes and Read Me files available in /usr/share/doc/ofed-docs-1.4.1/ after installation.

These updated packages also fix the following bugs:

- preloading the SDP protocol decreased performance significantly. The kernel and the userspace SDP protocol components have been updated, improving performance. (BZ#230034 , BZ#451471)
- the latest libsdp package appeared older than the previously-installed package because it was missing epoch information. This prevented upgrades to the latest package. This has been corrected, enabling upgrades. (BZ#448733)

- compat-dapl-utils was not permitted to access the its configuration information. This package now has its own dat.conf file, which resolves the issue and ensures that other sensitive data in the previous configuration file remains secure. (BZ#479942)
- dapl-utils and compat-dapl-utils did not trigger installation of all required dependencies at installation time, so installation failed. Each package now requires the libiverbs-driver (in all low-level packages) so all drivers are installed. Selecting the correct driver for specific hardware is the user's responsibility. (BZ#479943)
- administration of the RDS (Radio Data System) protocol, a kernel-level protocol, requires a tools package (rds-tools) that was not previously supported in Red Hat Enterprise Linux. Support for this package has been added, enabling RDS administration. (BZ#486978)
- the rds-tools-debuginfo package was empty, which prevented debugging. The package has been updated with debug information. (BZ#500627)
- valgrind exposed a number of errors when used to debug libraries that used a certain kind of mapped memory. These libraries will now be built with the --with-valgrind option to prevent this. (BZ#504284)
- valgrind could write data incorrectly to control registers for certain hardware types. This method is now explicitly banned. (BZ#505553)
- preliminary XRC support has been removed to cater for upstream API changes likely to break existing support. (BZ#506258)
- the order of Infiniband loading modules has been changed to prevent a conflict and EEH Recovery failure. (BZ#512777)
- when connected mode and IP bonding were used on IPoIB interfaces, the ifup_ib script exited before setting the connected mode or Maximum Transmission Unit (MTU) parameter. The processes that set the mode and the MTU parameter now occur earlier so that bonded interfaces will receive the mode and MTU parameter before ifup_ib exits. (BZ#513195)
- initscripts have been rewritten to include multi-protocol support for Mellanox ConnectX hardware. Ports can now be configured to operate in either Infiniband or 10 Gigabyte Ethernet mode. (BZ#460207)
- support for the Infiniband bonding tool has been added to allow bonding over IPoIB interfaces, which enables improved load-balancing and aggregation performance. (BZ#475663)
- mvapich has been updated to the current upstream release, and the build process has been altered to provide support for building and implementing Fortran 90-based modules. (BZ#479933 , BZ#479935)
- support for Mellanox 10 Gigabyte Ethernet hardware (MT25408 IB), as provided by the latest upstream OFED driver, has been added. (BZ#488114)
- userspace support for the new PCI device ID for the Chelsio S310e-CR iWARP/RDMA adapter is now enabled. (BZ#513226)

All Infiniband/iWARP hardware users are advised to upgrade to these re-based packages.

1.163. openoffice.org

1.163.1. RHBA-2009:1248: bug fix update

Updated openoffice.org packages that fix various bugs are now available.

OpenOffice.org is an Open Source, multi-platform office productivity suite. It includes key desktop applications, such as a word processor, spreadsheet, and presentation manager.

These updated openoffice.org packages fixes the following bugs:

Math would attempt to load an icon that was not a 24-bit image. This would result in a `pBitmap->mnBitCount == 24' warning message. OpenOffice.org now converts icons into 24-bit bitmaps, and launches successfully. (BZ#456845)

- Red Hat Enterprise Linux 5.0 did not support the '-headless' switch when launching OpenOffice.org. Partly as a consequence, OpenOffice.org was not configured for the Gnome desktop environment: launching would fail with a 'Can't open display' error. OpenOffice.org has now been updated to use GTK, and 'ooffice -headless' launches as expected. (BZ#461984)
- when exporting to a .rtf file, OpenOffice.org would make adjustments only for the UCS-2 encoding. Consequently, exporting when using the ja_JP locale would result in a .rtf file with erroneous characters. OpenOffice.org now adjusts for all encodings, and exports to .rtf as expected. (BZ#462055)
- long lines of Chinese text were not being shortened for the undo tooltip, resulting in an unattractive tooltip. OpenOffice.org now shortens these lines to be displayed as expected. (BZ#469145)
- OpenOffice.org was not checking file paths during the FileRename operation. Identical paths would cause the automated TestTool to crash. OpenOffice.org now aborts the operation for identical paths, and TestTool runs as expected. (BZ#469302)
- TestTool had not been updated to use new .odb files. Consequently, some test scripts would fail. TestTool has now been updated to use the new .odb files. (BZ#469321)
- Euro Converter did not recognize .sxc files, resulting in a conversion failure. Backwards compatibility has now been added and the tool can use .sxc files. (BZ#469330)
- Draw could not import Metafile images from a shell prompt; doing so would cause Draw to quit. Support for these image types has been improved in OpenOffice.org, and Draw now imports them correctly. (BZ#469615)
- the Next button in the Function Wizard was occasionally not being disabled. This resulted in confusing navigation. OpenOffice.org has been updated to disable the button, making usage clearer. (BZ#469630)
- numbered lists in HTML files were being imported incorrectly, resulting in a crash. OpenOffice.org now checks imported numbered lists for irregularities, so HTML files can import successfully. (BZ#469990)
- the 'refresh this document' property for .odp files was not being set properly. As a result, the property would always be '1 second'. OpenOffice.org now sets the property correctly, and it updates as expected. (BZ#470210)
- 'psprint.conf' was not being flagged as a configuration file. As a result, upgrading openoffice.org-core caused OpenOffice.org's printer configuration to be overwritten. The spec file now flags the file, ensuring it is not overwritten. (BZ#476221)
- Tables of Contents in .doc files only cover a maximum of 9 levels, while in OpenOffice.org files they cover 10. Consequently, files exported to .doc would not import again with the correct levels. OpenOffice.org has been updated to export with a cut-off of 9 levels, and .doc files now import and export correctly. (BZ#476959)
- when a print dialog box was closed it would be hidden but not released. The hidden dialog box would continue to poll the CUPS, causing a heavy server load. OpenOffice.org has been updated to release the dialog box properly to avoid polling the CUPS heavily. (BZ#480369)
- when OpenOffice.org opened a document containing tables it did not check how many rows were allowed. This could cause the application to crash. OpenOffice.org now checks the allowed rows until it reaches the end of the table frame. Documents with tables now open as expected. (BZ#480829)

OpenOffice.org users should upgrade to these updated packages, which resolve these issues.

1.164. openssh

1.164.1. RHSA-2009:1287: Low security, bug fix, and enhancement update

Updated openssh packages that fix a security issue, a bug, and add enhancements are now available for Red Hat Enterprise Linux 5.

This update has been rated as having low security impact by the Red Hat Security Response Team.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

A flaw was found in the SSH protocol. An attacker able to perform a man-in-the-middle attack may be able to obtain a portion of plain text from an arbitrary ciphertext block when a CBC mode cipher was used to encrypt SSH communication. This update helps mitigate this attack: OpenSSH clients and servers now prefer CTR mode ciphers to CBC mode, and the OpenSSH server now reads SSH packets up to their full possible length when corruption is detected, rather than reporting errors early, reducing the possibility of successful plain text recovery. (CVE-2008-5161)

This update also fixes the following bug:

- the ssh client hung when trying to close a session in which a background process still held tty file descriptors open. With this update, this so-called "hang on exit" error no longer occurs and the ssh client closes the session immediately. (BZ#454812)

In addition, this update adds the following enhancements:

- the SFTP server can now chroot users to various directories, including a user's home directory, after log in. A new configuration option -- ChrootDirectory -- has been added to "/etc/ssh/sshd_config" for setting this up (the default is not to chroot users). Details regarding configuring this new option are in the sshd_config(5) manual page. (BZ#440240)
- the executables which are part of the OpenSSH FIPS module which is being validated will check their integrity and report their FIPS mode status to the system log or to the terminal. (BZ#467268 , BZ#492363)

All OpenSSH users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues and add these enhancements. After installing this update, the OpenSSH server daemon (sshd) will be restarted automatically.

1.165. openssl

1.165.1. RHSA-2009:1335: Moderate security, bug fix, and enhancement update

Updated openssl packages that fix several security issues, various bugs, and add enhancements are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

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. Datagram TLS (DTLS) is a protocol based on TLS that is capable of securing datagram transport (for example, UDP).

Multiple denial of service flaws were discovered in OpenSSL's DTLS implementation. A remote attacker could use these flaws to cause a DTLS server to use excessive amounts of memory, or crash on an invalid memory access or NULL pointer dereference. (CVE-2009-1377, CVE-2009-1378, CVE-2009-1379, CVE-2009-1386, CVE-2009-1387)

Note: These flaws only affect applications that use DTLS. Red Hat does not ship any DTLS client or server applications in Red Hat Enterprise Linux.

An input validation flaw was found in the handling of the BMPString and UniversalString ASN1 string types in OpenSSL's ASN1_STRING_print_ex() function. An attacker could use this flaw to create a specially-crafted X.509 certificate that could cause applications using the affected function to crash when printing certificate contents. (CVE-2009-0590)

Note: The affected function is rarely used. No application shipped with Red Hat Enterprise Linux calls this function, for example.

These updated packages also fix the following bugs:

- "openssl smime -verify -in" verifies the signature of the input file and the "-verify" switch expects a signed or encrypted input file. Previously, running openssl on an S/MIME file that was not encrypted or signed caused openssl to segfault. With this update, the input file is now checked for a signature or encryption. Consequently, openssl now returns an error and quits when attempting to verify an unencrypted or unsigned S/MIME file. (BZ#472440)
- when generating RSA keys, pairwise tests were called even in non-FIPS mode. This prevented small keys from being generated. With this update, generating keys in non-FIPS mode no longer calls the pairwise tests and keys as small as 32-bits can be generated in this mode. Note: In FIPS mode, pairwise tests are still called and keys generated in this mode must still be 1024-bits or larger. (BZ#479817)

As well, these updated packages add the following enhancements:

- both the libcrypto and libssl shared libraries, which are part of the OpenSSL FIPS module, are now checked for integrity on initialization of FIPS mode. (BZ#475798)
- an issuing Certificate Authority (CA) allows multiple certificate templates to inherit the CA's Common Name (CN). Because this CN is used as a unique identifier, each template had to have its own Certificate Revocation List (CRL). With this update, multiple CRLs with the same subject name can now be stored in a X509_STORE structure, with their signature field being used to distinguish between them. (BZ#457134)
- the fipscheck library is no longer needed for rebuilding the openssl source RPM. (BZ#475798)

OpenSSL users should upgrade to these updated packages, which resolve these issues and add these enhancements.

1.166. openswan

1.166.1. RHSA-2009:1138: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1138

Updated openswan packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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. Everything passing through the untrusted network is encrypted by the IPsec gateway machine, and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network (VPN).

Multiple insufficient input validation flaws were found in the way Openswan's pluto IKE daemon processed some fields of X.509 certificates. A remote attacker could provide a specially-crafted X.509 certificate that would crash the pluto daemon. (CVE-2009-2185)

All users of openswan are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. After installing this update, the ipsec service will be restarted automatically.

1.166.2. RHSA-2009:0402: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0402

Updated openswan packages that fix various security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

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. Everything passing through the untrusted network is encrypted by the IPsec gateway machine, and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network (VPN).

Gerd v. Egidy discovered a flaw in the Dead Peer Detection (DPD) in Openswan's pluto IKE daemon. A remote attacker could use a malicious DPD packet to crash the pluto daemon. (CVE-2009-0790)

It was discovered that Openswan's livetest script created temporary files in an insecure manner. A local attacker could use this flaw to overwrite arbitrary files owned by the user running the script. (CVE-2008-4190)

Note: The livetest script is an incomplete feature and was not automatically executed by any other script distributed with Openswan, or intended to be used at all, as was documented in its man page. In these updated packages, the script only prints an informative message and exits immediately when run.

All users of openswan are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the ipsec service will be restarted automatically.

1.166.3. RHEA-2009:1350: bug fix update

An updated openswan package that resolves several issues and provides FIPS-1402-2 compliance is now available.

Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN.

This package contains the daemons and userland tools for setting up Openswan. It optionally also builds the Openswan KLIPS IPsec stack that is an alternative for the NETKEY/XFRM IPsec stack that exists in the default Linux kernel.

Openswan 2.6.x also supports IKEv2 (RFC 4309)

Bugs fixed in these updated packages include:

- Openswan would not allow IPsec connections between a physical IP on one system and a virtual IP on another system if the physical IP on the first system was already connected to the physical IP on the second system that was associated with that virtual IP. Now, Openswan creates a new route if a route already exists. This allows simultaneous IPsec connections to a physical IP and the virtual IP associated with it. (BZ#438998)
- the parser in lib/libipsecconf/ does not correctly interpret values supplied in manual keyring, and the use of the manual keyring could therefore result in a segmentation fault in Openswan. Because the manual keyring is no longer supported, Openswan will now exit with an error when ipsec manual up <connection-name> is used. (BZ#449725)
- the ipsec.conf file included any .conf files placed in /etc/ipsec.d but Openswan's default installation did not place any files in this directory. Therefore, error messages similar to "could not open include filename: '/etc/ipsec.d/*.conf"' would appear when starting or stopping the IPsec service. Although the service operated correctly, the appearance of these error messages could mislead a user to think that there was a problem with IPsec. The ipsec.conf file now comments out the include of /etc/ipsec.d and contains a note suggesting that users uncomment the line and use /etc/ipsec.d for their customized configuration files. (BZ#463931)
- Openswan did not close file decriptors on exec. The resulting file descriptor leaks would then cause AVC denial warnings on systems set to enforce SELinux policy. Openswan now closes file descriptors on exec, both for sockets that it has opened and for sockets that it has accepted. Because Openswan does not now leak these file descriptors, the corresponding AVC denial warnings do not appear. (BZ#466861)
- Openswan's cryptographic methods did not meet the standards for FIPS 140-2 certification, therefore precluding the use of Openswan in environments that require this certification. Openswan now uses the NSS library and includes:
  - encryption/decryption algorithms (AES, 3DES)
  - hash and data integrity algorithm (MD5, SHA1, SHA2(256, 384, 512))
  - HMAC mechanisms for the above hash algorithms.
  - authentication with signature (without certificates) (DS_AUTH). Specifically, it uses RSA signatures.
  - authentication with signature (with x.509 certificates) (DS_AUTH).
  - Oakley Diffie-Hellman (DH) related cryptographic operations.
  - random number generation through NSS.
  - support for NSS DB without and with password.
  - FIPS integrity check using fipscheck library
  - support for old (dbm) and new (sql) NSS databases (dbm)
- Openswan now meets the FIPS 140-2 standard. (BZ#444801 , BZ#469763)
- previously, the package description included a reference to a "freeswan enabled kernel". This reference could have mislead users into thinking that Openswan required some special kernel, when no such kernel exists. The reference has therefore been removed, eliminating the potential for confusion. (BZ#487708)

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

1.167. oprofile

1.167.1. RHBA-2009:1322: bug fix and enhancement update

An updated oprofile package that adds support for the Java just-in-time runtime environment and fixes an opcontrol bug is now available.

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 makes use of the hardware performance counters provided on many processors, and can use the Real Time Clock (RTC) for profiling on processors without counters.

This update applies the following fixes:

- A bug that prevented opcontrol from displaying the 'Parameters' field whenever the --verbose option was used is now fixed. In previous releases, opcontrol incorrectly used the do_init shell function to initialize the VERBOSE variable (which contained the parameter list) to NULL. With this update, opcontrol now uses the do_option shell function to initialize the VERBOSE variable. (BZ#454969)
- This update also provides support for collecting data on programs using Java runtime environments that support jvmti (Java 1.5.0 and newer). (BZ#474666)

Users of oprofile are advised to upgrade to this update.

1.168. pam

1.168.1. RHBA-2009:1358: bug fix and enhancement update

Updated pam packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

Pluggable Authentication Modules (PAM) provide a system whereby administrators can set up authentication policies without having to recompile programs that handle authentication.

These updated pam packages provide fixes for the following bugs:

- when called from a screensaver running under a non-zero UserID, the pam_tally2 module could repeatedly prompt for the user's password and then log the following error to syslog: "Error opening /var/log/tallylog for update: Permission denied". With this update, pam_tally2 correctly ignores failures to open the tallylog in this situation. (BZ#429169)
- the pam_access module unnecessarily attempted to resolve entries listed in the access.conf file through DNS lookups, even if the service was not called from a network. The pam_access module has been changed so that it does not attempt to resolve the origins of entries in access.conf which do not contain an IP address or an IP addresses and a netmask value. (BZ#459057)
- the pam_keyinit module did not save the UserID (UID) of the process during session close, which made it unable to switch back to that original UID. An error message was output to the system log in that case. The UID is now correctly saved with these updated packages, which makes the spurious log message disappear. (BZ#466411)
- the pam_filter module was not able to open a new pseudoterminal, which prevented the module from functioning properly. With this update, pam_filter is able to open new pseudoterminals. (BZ#473970)
- when the "open_tty" module was used in combination with the "pam_tty_audit" module in the system-auth pam configuration file, pam_tty_audit could segmentation fault if the "open_only" option was set and the open_tty module was called by the "su" command or another utility. (BZ#476833)

- the "smbpasswd" utility allows a user to change their encrypted SMB password, which is stored in the smbpasswd file. However, it was not possible for non-root users to change their password with "smbpasswd" due to overly strict checking in the helper of the pam_unix module. This has been corrected so that users can once again change their SMB passwords using "smbpasswd". (BZ#476904)

- the coreutils package was listed incorrectly as a prerequisite requirement for the pam packages instead of a post-install requirement. This dependency statement has been corrected in these updated packages. (BZ#497570)

In addition, these updated packages provide the following enhancements:

- Gnome Display Manager's (GDM's) accessibility features did not function correctly when an audio device was not properly configured. The configuration file for console device modes now sets audio devices as owned by the "audio" group if there is no console user. This provides support for accessible login with GDM. (BZ#244688)

- the pam_tally2 module now supports a new option that allows serialized access to the /var/log/tallylog file. Enabling this option prevents possible failed authentication when two separate processes attempt to authenticate nearly simultaneously when the lock_time option ("always deny for n seconds after a failed attempt") is set to a value of one or greater. (BZ#455217)

- these updated pam packages provide a new PAM module, pam_faildelay, which can read the "FAIL_DELAY" value from the /etc/login.defs configuration file and set the amount of delay between login prompts following a failed login attempt to that value. (BZ#476217)

- these updated pam packages provide a new PAM module, pam_pwhistory, which saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently. (BZ#451085)

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

1.169. pango

1.169.1. RHSA-2009:0476: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0476

Updated pango and evolution28-pango packages that fix an integer overflow flaw are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Pango is a library used for the layout and rendering of internationalized text.

Will Drewry discovered an integer overflow flaw in Pango's pango_glyph_string_set_size() function. If an attacker is able to pass an arbitrarily long string to Pango, it may be possible to execute arbitrary code with the permissions of the application calling Pango. (CVE-2009-1194)

pango and evolution28-pango users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, you must restart your system or restart the X server for the update to take effect. Note: Restarting the X server closes all open applications and logs you out of your session.

1.169.2. RHBA-2009:1395: bug fix update

An updated Pango package that rectifies a dependency issue is now available.

Pango is a library for laying out and rendering of text, with an emphasis on internationalization. Pango can be used anywhere that text layout is needed, though most of the work on Pango so far has been done in the context of the GTK+ widget toolkit. Pango forms the core of text and font handling for GTK+.

Pango is designed to be modular; the core Pango layout engine can be used with different font back-ends.

The integration of Pango with Cairo provides a complete solution with high quality text handling and graphics rendering.

This update addresses the following bug:

- it was possible to install Pango (and applications that relied upon Pango), without having any fonts installed. This would prevent applications from loading (as they could not render text) and resulted in an error message. Changes have been made to ensure that the bitsream-vera-fonts package is now a dependency of Pango. With the font present, applications reliant upon Pango can load and render text correctly. (BZ#251928)

User should upgrade to the updated package, which resolves this issue.

1.170. pciutils

1.170.1. RHBA-2009:1110: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1110

An updated pciutils package that fixes a bug is now available.

The pciutils package contains various utilities for inspecting and manipulating devices connected to the PCI bus.

This updated pciutils package fixes the following bug:

- using the command "lspci -v" on a system which contained an AD167A Emulex Fibre Channel card caused continuous output. This updated pciutils package contains a fix for this bug so that the output from calling "lspci -v" on systems with this Fibre Channel card always terminates successfully. (BZ#487208)

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

1.171. perl

1.171.1. RHBA-2009:0406: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0406

An updated perl package that fixes a bug is now available.

Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text.

These updated perl packages provide a fix for the following bug:

- the Time::HiRes Perl module is incompatible with the latest version of glibc, which caused setitimer errors to be written to /var/log/dmesg when the alarm() function of HiRes was called with a time greater than one second. With this update, the Time::HiRes module calls setitimer with the correct parameters and no error messages are written to /var/log/dmesg, thus resolving this issue.

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

1.171.2. RHBA-2009:1244: bug fix and enhancement update

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

Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text.

These updated perl packages provide fixes for the following bugs:

- the Time::HiRes Perl module is incompatible with the latest version of glibc, which caused setitimer errors to be written to /var/log/dmesg when the alarm() function of HiRes was called with a time greater than one second. With this update, the Time::HiRes module calls setitimer with the correct parameters and no error messages are written to /var/log/dmesg, thus resolving this issue. (BZ#453327)

- on multilib systems such as AMD64, the libnet.cfg Perl configuration file, which controls whether CPAN requests use active or passive FTP, was located in the /usr/lib64/perl5/5.8.5/Net/ directory, where it had no effect. This has been corrected with this update: libnet.cfg is now located in the /usr/lib/perl5/5.8.5/Net/ directory, where its active/passive FTP settings properly affect CPAN requests. (BZ#490107)

- the @INC array is a list of directories that Perl searches when attempting to load modules. The @INC array became quite large, which negatively affected performance and led to verbose error messages. Instead of adding all search paths to the @INC array, this update populates it only with those paths which actually do exist at the startup of the interpreter, thus culling nonexistent paths. In this way, performance is improved and compatibility with installations of older modules is retained. (BZ#489909)

In addition, these updated packages provide the following enhancements:

- the File::Temp module has been updated to version 0.18. (BZ#458851)

- the Scalar::Util and List::Util modules have been updated to version 1.21. (BZ#507378)

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

1.172. perl-DBD-Pg

1.172.1. RHSA-2009:0479: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0479

An updated perl-DBD-Pg package that fixes two security issues is now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Perl DBI is a database access Application Programming Interface (API) for the Perl language. perl-DBD-Pg allows Perl applications to access PostgreSQL database servers.

A heap-based buffer overflow flaw was discovered in the pg_getline function implementation. If the pg_getline or getline functions read large, untrusted records from a database, it could cause an application using these functions to crash or, possibly, execute arbitrary code. (CVE-2009-0663)

Note: After installing this update, pg_getline may return more data than specified by its second argument, as this argument will be ignored. This is consistent with current upstream behavior. Previously, the length limit (the second argument) was not enforced, allowing a buffer overflow.

A memory leak flaw was found in the function performing the de-quoting of BYTEA type values acquired from a database. An attacker able to cause an application using perl-DBD-Pg to perform a large number of SQL queries returning BYTEA records, could cause the application to use excessive amounts of memory or, possibly, crash. (CVE-2009-1341)

All users of perl-DBD-Pg are advised to upgrade to this updated package, which contains backported patches to fix these issues. Applications using perl-DBD-Pg must be restarted for the update to take effect.

1.173. php

1.173.1. RHSA-2009:0338: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0338

Updated php packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Web server.

A heap-based buffer overflow flaw was found in PHP's mbstring extension. A remote attacker able to pass arbitrary input to a PHP script using mbstring conversion functions could cause the PHP interpreter to crash or, possibly, execute arbitrary code. (CVE-2008-5557)

A flaw was found in the handling of the "mbstring.func_overload" configuration setting. A value set for one virtual host, or in a user's .htaccess file, was incorrectly applied to other virtual hosts on the same server, causing the handling of multibyte character strings to not work correctly. (CVE-2009-0754)

A buffer overflow flaw was found in PHP's imageloadfont function. If a PHP script allowed a remote attacker to load a carefully crafted font file, it could cause the PHP interpreter to crash or, possibly, execute arbitrary code. (CVE-2008-3658)

A flaw was found in the way PHP handled certain file extensions when running in FastCGI mode. If the PHP interpreter was being executed via FastCGI, a remote attacker could create a request which would cause the PHP interpreter to crash. (CVE-2008-3660)

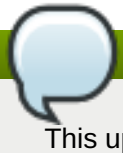
A memory disclosure flaw was found in the PHP gd extension's imagerotate function. A remote attacker able to pass arbitrary values as the "background color" argument of the function could, possibly, view portions of the PHP interpreter's memory. (CVE-2008-5498)

A cross-site scripting flaw was found in a way PHP reported errors for invalid cookies. If the PHP interpreter had "display_errors" enabled, a remote attacker able to set a specially-crafted cookie on a victim's system could possibly inject arbitrary HTML into an error message generated by PHP. (CVE-2008-5814)

All php users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. The httpd web server must be restarted for the changes to take effect.

1.174. php-pear

1.174.1. RHBA-2009:1071: bug fix update



Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1071

An updated php-pear package that fixes various bugs is now available.

The PHP Extension and Application Repository (PEAR) is a framework and distribution system for reusable PHP components.

This updated php-pear package includes fixes for the following bugs:

- installing certain PHP components using the /usr/bin/pecl command resulted in failures and error message similar to the following:

  ```
  Fatal error: Allowed memory size of [amount] bytes exhausted
  ```

  This updated php-pear package increases the amount of system memory available to the /usr/bin/pecl command with the result that PHP components which previously failed to install due to out-of-memory errors now install cleanly and without error. (BZ#460072)

- attempting to install a PHP component using PEAR's /usr/bin/pecl command resulted in an error message stating that pecl needed access to the "phpize" command, and therefore could not continue with the install. The phpize utility is used to prepare the build environment for a PHP extension. This issue has been resolved by adding a dependency on the php-devel package to the php-pear package, with the result that installing components with pecl should now complete as expected, and without having to chase any further dependencies. (BZ#482974)

- the /usr/bin/pear command emitted warnings when the global "error_reporting" PHP configuration variable was set to the value "E_STRICT". The E_STRICT error-reporting level was introduced into PHP and PEAR following the release of PHP 5, and has the aim of ensuring that the package is strictly PHP 5-

compatible. With this updated package, /usr/bin/pear no longer emits warnings when the error-reporting level is set to E_STRICT. (BZ#461142)

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

1.175. pidgin

1.175.1. RHSA-2009:1218: Critical security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1218

Updated pidgin packages that fix a security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Pidgin is an instant messaging program which can log in to multiple accounts on multiple instant messaging networks simultaneously.

Federico Muttis of Core Security Technologies discovered a flaw in Pidgin's MSN protocol handler. If a user received a malicious MSN message, it was possible to execute arbitrary code with the permissions of the user running Pidgin. (CVE-2009-2694)

Note: Users can change their privacy settings to only allow messages from users on their buddy list to limit the impact of this flaw.

These packages upgrade Pidgin to version 2.5.9. Refer to the Pidgin release notes for a full list of changes: http://developer.pidgin.im/wiki/ChangeLog

All Pidgin users should upgrade to these updated packages, which resolve this issue. Pidgin must be restarted for this update to take effect.

1.175.2. RHSA-2009:1139: Moderate security and bug fix update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1139

Updated pidgin packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Pidgin is an instant messaging program which can log in to multiple accounts on multiple instant messaging networks simultaneously. The AOL Open System for CommunicAtion in Realtime (OSCAR) protocol is used by the AOL ICQ and AIM instant messaging systems.

A denial of service flaw was found in the Pidgin OSCAR protocol implementation. If a remote ICQ user sent a web message to a local Pidgin user using this protocol, it would cause excessive memory usage, leading to a denial of service (Pidgin crash). (CVE-2009-1889)

These updated packages also fix the following bug:

- the Yahoo! Messenger Protocol changed, making it incompatible (and unusable) with Pidgin versions prior to 2.5.7. This update provides Pidgin 2.5.8, which implements version 16 of the Yahoo! Messenger Protocol, which resolves this issue.

Note

These packages upgrade Pidgin to version 2.5.8. Refer to the Pidgin release notes for a full list of changes: http://developer.pidgin.im/wiki/ChangeLog

All Pidgin users should upgrade to these updated packages, which correct these issues. Pidgin must be restarted for this update to take effect.

1.175.3. RHBA-2009:0407: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0407

Updated Pidgin packages that fix significant bugs are now available for Red Hat Enterprise Linux 4 and 5.

Pidgin is a multi-protocol Internet Messaging (IM) client.

This update addresses the following bugs:

- the ICQ Internet message protocol servers recently changed and now require clients to use a newer version of the ICQ protocol. When logging in to ICQ Pidgin 2.5.2 (the version previously shipped with Red Hat Enterprise Linux 4 and 5) fails with an error message as a result. Pidgin 2.5.5, included with this update, uses the newer ICQ protocol, which resolves this issue. (BZ#490104 , BZ#490094)

  Note

  Pidgin 2.5.5 also addresses several other minor bugs. See the Pidgin 2.5.5 ChangeLog, for details regarding these other changes.

- users with "One-Time Password" authenticated logins reported authentication failures because Pidgin attempts to re-connect using the previous password after disconnecting from an IM service. This behavior presented even if the "Remember password" check-box was unchecked in the Account Editor dialog box for a given account (Choose Accounts > Manage Accounts to open a list of active accounts. Double-click an account on this list to show the Account Editor dialog box for that account.)

A new plug-in, "One Time Password Support", is included with this update. With this plug-in enabled, a "One-Time Password" checkbox appears in the Advanced tab of the Account Editor dialog box. For each account that requires One-Time Password authentication, check this checkbox in the Advanced tab. You must also uncheck the "Remember password" checkbox in the Basic tab for this plug-in to work. (BZ#490536 , BZ#490539)

Note

because of the unpredictable disconnection rate for IM sessions, the attempts to automatically re-connect noted above are by design and are not considered a bug. The One Time Password plug-in allows the enforcement, on a per-account basis, of One-Time Password authentication. With the plug-in active, Pidgin will still attempt to re-connect to services after being disconnected. It will not, however, use the previous password.

All Pidgin users should upgrade to these updated packages, which contains Pidgin version 2.5.5 and resolves these issues. Note: after these errata packages are installed, Pidgin must be restarted for the update to take effect.

1.176. piranha

1.176.1. RHBA-2009:1396: bug-fix update

Updated piranha packages that fix several bugs are now available.

Piranha provides high-availability and load balancing services for Red Hat Enterprise Linux. It includes various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism, that provides load balancing, primarily for Web and FTP servers.

This update fixes the following bugs:

- Logrotate rotates all files including previously rotated one.
- Nanny does not default to webservice query string when no query/expect string specified.
- Piranha-gui removes slashes from monitoring script send commands.
- Adding real port in piranha-gui caused pulse to error.

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

1.177. policycoreutils

1.177.1. RHBA-2009:1292: bug fix update

Updated policycoreutils packages that fix several bugs are now available.

policycoreutils contains the policy core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system. These utilities include load_policy to load policies, setfiles to label file systems, newrole to switch roles, and run_init to run "/etc/init.d/" scripts in the proper context.

These updated packages fix the following bugs:

- when attempting to change contexts, chcat reported invalid argument and insufficient space errors because of a limit to the number of extended attributes that could be included as an argument. This update fixes the issue. (BZ#220813)
- executing the "semanage port -{a|d|m} [-tr] [-p protocol] port" command failed if SELinux was disabled. This update adds support for selecting a store with semanage so that application policies can be updated when SELinux is disabled. (BZ#316011)

- genhomedircon could not process a HOME_DIR with a context <<none>>. This condition has been added and the problem has been resolved. (BZ#354361)
- restorecond.conf did not include definitions for ~/web or ~/www directories. The paths for these directories have been added to restorecond.conf, resolving this issue. (BZ#458687)
- chcat did not translate category IDs to name strings when a user belonged to multiple categories. chcat and setrans.conf have been modified so that category IDs are translated as expected on all architectures and the error no longer presents. (BZ#459677)
- clicking on the table header in system-config-selinux network port view should have toggled numerical sorting of values, but did not activate the sort method. This update fixes the sort order action for the ports page. (BZ#468170)
- policycoreutils did not support the use of "semodule -DB" when removing dontaudit messages. Upstream "semodule -DB" support has been added so that users have a simple mechanism to remove all dontaudit rules while building policies. (BZ#493115)

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

1.178. poppler

1.178.1. RHSA-2009:0480: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0480

Updated poppler packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Poppler is a Portable Document Format (PDF) rendering library, used by applications such as Evince.

Multiple integer overflow flaws were found in poppler. An attacker could create a malicious PDF file that would cause applications that use poppler (such as Evince) to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0147, CVE-2009-1179, CVE-2009-1187, CVE-2009-1188)

Multiple buffer overflow flaws were found in poppler's JBIG2 decoder. An attacker could create a malicious PDF file that would cause applications that use poppler (such as Evince) to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0146, CVE-2009-1182)

Multiple flaws were found in poppler's JBIG2 decoder that could lead to the freeing of arbitrary memory. An attacker could create a malicious PDF file that would cause applications that use poppler (such as Evince) to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0166, CVE-2009-1180)

Multiple input validation flaws were found in poppler's JBIG2 decoder. An attacker could create a malicious PDF file that would cause applications that use poppler (such as Evince) to crash or, potentially, execute arbitrary code when opened. (CVE-2009-0800)

Multiple denial of service flaws were found in poppler's JBIG2 decoder. An attacker could create a malicious PDF file that would cause applications that use poppler (such as Evince) to crash when opened. (CVE-2009-0799, CVE-2009-1181, CVE-2009-1183)

Red Hat would like to thank Braden Thomas and Drew Yao of the Apple Product Security team, and Will

Dormann of the CERT/CC for responsibly reporting these flaws.

Users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

1.179. ppc64-utils

1.179.1. RHEA-2009:1247: enhancement update

Enhanced ppc64-utils packages that add support for virtual Fibre Channel devices to the ofpathname script are now available.

ppc64-utils is a collection of utilities for Linux running on 64-bit PowerPC platforms.

These updated ppc64-utils packages add the following enhancement:

- previously, the ofpathname script was not able to translate logical device names to Open Firmware device path names for virtual Fibre Channel devices. With these updated packages, ofpathname now supports virtual Fibre Channel devices. For more information on ofpathname, refer to the ofpathname(8) manual page. (BZ#477201)

Users of ppc64-utils are advised to upgrade to these updated packages, which add this enhancement.

1.180. psmisc

1.180.1. RHBA-2009:0439: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0439

An updated psmisc package that fixes a bug is now available.

The psmisc package contains utilities for managing processes on your system: pstree, killall, and fuser. The pstree command displays a tree structure of all of the running processes on your system. The killall command sends a specified signal (SIGTERM if nothing is specified) to processes identified by name. The fuser command identifies the PIDs of processes that are using specified files or file systems.

This updated psmisc package fixes the following bug:

- calling the command "fuser -m <device>" failed to detect open files on a file system that had been lazily unmounted (by calling "umount -l <device>", for example). The fuser utility detects open files on lazily-unmounted file systems with this updated package.

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

1.181. pykickstart

1.181.1. RHBA-2009:1387: bug fix update

An updated pykickstart package that fixes two bugs is now available.

The pykickstart package is a python library used to manipulate kickstart files.

This updated package addresses the following bugs:

- pykickstart ignored special characters when parsing arguments, and therefore omitted them when passing the arguments to the authconfig method. This meant that the system would not kickstart as specified. pykickstart now handles special characters, so arguments are passed as intended. Any further issues will be due to incorrect syntax. (BZ#241657)
- pykickstart lacked RAID10 support, so attempting to kickstart with RAID10 software resulted in a "RAID Partition defined without RAID level" error message and a failure to boot. RAID10 support has been added, and the kickstart now works as expected. (BZ#508053)

Users of pykickstart are advised to upgrade to this updated package, which fixes these issues.

1.182. pyorbit

1.182.1. RHBA-2009:1056: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1056

An updated pyorbit package that fixes a bug is now available.

pyorbit is an extension module for python that gives you access to the ORBit2 CORBA ORB.

This updated package addresses the following bug:

- CORBA object typecodes were being ignored when querying objects from sources other than ORBit, such as Java. Pyorbit now checks typecode to find stubs for non-ORBit objects, and includes binary compatibility from upstream modules. (BZ#244921)

Users should upgrade to this updated package, which resolves the issue.

1.183. python

1.183.1. RHSA-2009:1176: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1176

Updated python packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Python is an interpreted, interactive, object-oriented programming language.

When the assert() system call was disabled, an input sanitization flaw was revealed in the Python string

object implementation that led to a buffer overflow. The missing check for negative size values meant the Python memory allocator could allocate less memory than expected. This could result in arbitrary code execution with the Python interpreter's privileges. (CVE-2008-1887)

Multiple buffer and integer overflow flaws were found in the Python Unicode string processing and in the Python Unicode and string object implementations. An attacker could use these flaws to cause a denial of service (Python application crash). (CVE-2008-3142, CVE-2008-5031)

Multiple integer overflow flaws were found in the Python imageop module. If a Python application used the imageop module to process untrusted images, it could cause the application to disclose sensitive information, crash or, potentially, execute arbitrary code with the Python interpreter's privileges. (CVE-2007-4965, CVE-2008-4864)

Multiple integer underflow and overflow flaws were found in the Python snprintf() wrapper implementation. An attacker could use these flaws to cause a denial of service (memory corruption). (CVE-2008-3144)

Multiple integer overflow flaws were found in various Python modules. An attacker could use these flaws to cause a denial of service (Python application crash). (CVE-2008-2315, CVE-2008-3143)

An integer signedness error, leading to a buffer overflow, was found in the Python zlib extension module. If a Python application requested the negative byte count be flushed for a decompression stream, it could cause the application to crash or, potentially, execute arbitrary code with the Python interpreter's privileges. (CVE-2008-1721)

A flaw was discovered in the strxfrm() function of the Python locale module. Strings generated by this function were not properly NULL-terminated, which could possibly cause disclosure of data stored in the memory of a Python application using this function. (CVE-2007-2052)

Red Hat would like to thank David Remahl of the Apple Product Security team for responsibly reporting the CVE-2008-2315 issue.

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

1.183.2. RHBA-2009:1402: bug fix update

Updated python packages that fix several thread and subprocess bugs are now available for Red Hat Enterprise Linux 5.

Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC).

These updated packages apply fixes for the following bugs:

- processes were cleaned and their IDs recycled regardless of whether the processes had an active reference. This meant that child processes had their IDs recycled before their parent called for a value, which resulted in an OS Error (No child processes). The parent now checks whether a child process has returned before cleaning its ID, and the error no longer presents. (BZ#498979 , BZ#498978)

- a child process would attempt to import variables that had already been imported by a parent process. This meant that both parent and child could attempt to import simultaneously, which could cause a deadlock between parent and child threads. Since the child process can inherit the variables of its parent, the child's import method has been removed and the process no longer hangs. (BZ#499095 , BZ#499097)

All users are advised to upgrade to these updated python packages, which contain the fixes for these issues.

1.184. python-pyblock

1.184.1. RHBA-2009:1319: bug fix update

An updated python-pyblock package that fixes a bug is now available.

The python-pyblock package contains python bindings for device-mapper functionalities; mainly dmraid and multipath.

This update addresses the following bug:

- pyblock activated and de-activated dmraid sets incorrectly (it did not activate the leaves first and it did not start de-activation with the root). This presented as anaconda being unable to install Red Hat Enterprise Linux 5 onto RAID10 arrays. With this update, pyblock deals with dmraid sets correctly and, consequently, Red Hat Enterprise Linux 5 installs as expected onto RAID10 arrays. (BZ#475386)

Users should upgrade to this updated package, which resolves this issue.

1.185. python-virtinst

1.185.1. RHBA-2009:1412:bug fix and enhancement update

An updated python-virtinst package that fixes bugs and adds enhancements is now available.

The python-virtinst package contains virtinst, a module to help start installations of Red Hat Enterprise Linux or Fedora inside a virtual machine. It supports para-virtualized and fully-virtualized guests. As well, the python-virtinst package contains a script, virt-install, which uses virtinst in a command-line mode.

This update addresses the following bugs:

- to install a virtual machine using a remote ISO, the "--cdrom" argument can take a Uniform Resource Indicator (URI) value. Previously this did not work, instead failing with a "Cannot create storage for cdrom device error. The re-base to version 0.400.3 (see below) includes a fix for this: giving a remote URI value to the "--cdrom" argument now works as expected. (BZ#506714)

- if installation of a virtual instance of Red Hat Enterprise Linux or Fedora took longer than the time specified by the "--wait" option, virt-installs exited and printed the error "Installation has exceeded specified timelimit. Aborting." Since the installation itself is not affected, "Aborting" has been edited to the clearer "Exiting application". (BZ#476717)

As well, this updated package includes the following enhancements:

- when creating a new guest, the default sound hardware was previously es1370 with the user able to select pcspk and sb16 as alternatives. For this update, ac97 has been added as an option for both Xen and KVM virtual machines. As well, for KVM virtual machines, ac97 is now the default choice (for Xen virtual machines the default remains es1370). (BZ#508747)

- to support KVM on Red Hat Enterprise Linux 5, python-virtinst was re-based from version 0.300.2 to version 0.400.3. (BZ#489375)

Along with KVM support, this re-base adds multiple new features, including:

- the new "virt-convert" tool. virt-convert allows conversion between different virtualization configuration file formats. Note: this currently only supports converting between vmx and virt-image formats.

- virt-install support for remote guest installations.

- the new "--disk" option for virt-install. This allows many more storage attributes via the command line, as well as libvirt storage specific information.
- the new "--sound" option for virt-install. This allows sound devices to be attached to guest operating systems.
- the new "--hostdev" option for virt-install. This allows a physical host device to be attached to guest operating systems.
- the new "--import" option for virt-install. This allows for the creation of a guest from an existing disk image, with no installation phase required.
- the virt-* tools no longer run interactively by default. The user must pass the --prompt option to force this mode. (Messages to STD OUT inform users familiar with the previous default of this new setting.) This was done to make the tools more friendly for scripting purposes.

Users of python-virtinst are advised to upgrade to this updated package, which fixes these issues and provides these enhancements.

1.186. resktop

1.186.1. RHEA-2009:1417: bug fix and enhancement update

An enhanced rdesktop package that fixes a bug is now available.

The rdesktop application is a client for Microsoft Windows NT Terminal Server, Windows 2000 Terminal Services, Windows 2003 Terminal Services/Remote Desktop, Windows XP Remote Desktop, and possibly other Terminal Services products. Currently, the Remote Desktop Protocol (RDP) version 4 and 5 protocols are implemented in rdesktop.

This update upgrades rdesktop to upstream version 1.6.0, which contains a number of bug fixes and enhancements over the previous version.

Notably, this updated rdesktop package adds the following enhancements:

- smart card-enabled login is now supported. (BZ#253307)
- support for Secure Sockets Layer (SSL) connections has been improved. (BZ#253307)
- support for connecting to Windows Vista hosts has been added. (BZ#459140, BZ#337231)

Also notably, the following bug has been fixed:

- when using rdesktop to connect to a Windows 2003 Terminal Server, rapid scrolling by the user in the Word or Excel applications caused the screen to refresh incorrectly. Minimizing and then restoring the affected application returned the screen to a correctly-refreshed state. This has been fixed with this updated package so that rapid scrolling does not cause screen refresh issues. (BZ#252023, BZ#218684)

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

1.187. readline

1.187.1. RHBA-2009:1078: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1078

An updated readline package that fixes a bug is now available.

The Readline library provides a set of functions that allow users to edit command lines.

This updated package fixes the following bug:

- readline failed to re-allocate the array used to keep track of wrapped screen lines. For a long enough input line, this resulted in an invalid pointer error and a segmentation fault crash. With this update, the array is properly re-allocated and the crash no longer occurs. (BZ#473359)

All Readline users should upgrade to this updated package, which resolves this issue.

1.188. redhat-release

1.188.1. RHEA-2009:1400: bug fix and enhancement update

A new redhat-release package is now available for Red Hat Enterprise Linux 5.4.

The redhat-release package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

This new package reflects changes made for the release of Red Hat Enterprise Linux 5.4.

Users of Red Hat Enterprise Linux 5 should upgrade to this updated package.

1.189. redhat-release-notes

1.189.1. RHEA-2009:1385: enhancement update

An enhanced redhat-release-notes package is now available.

An updated version of the redhat-release-notes package is now available as part of ongoing support and maintenance of Red Hat Enterprise Linux 5.

This package contains the release notes for Red Hat Enterprise Linux 5.4

1.190. redhat-rpm-config

1.190.1. RHBA-2009:1089: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1089

An updated redhat-rpm-config package that fixes a bug is now available.

redhat-rpm-config is a package that provides customized Red Hat macros used during the building of RPM packages. These macros replace the standard macros supplied as part of RPM itself with Red Hat specific versions.

This updated redhat-rpm-config package fixes the following bug:

- the "brp-java-repack-jars" script was unable to correctly handle certain Java ARchive files (JAR) files. Those files would set the permissions on exploded directory hierarchies to strange permissions modes, such as "0000". With this updated package, standard user permissions are set correctly on the exploded directory hierarchy, which prevents certain errors from occurring, such as being unable to remove the directory tree when it is necessary to do so. (BZ#219706)

All users of redhat-rpm-config are advised to upgrade to this updated package, which resolves this issue.

1.191. rgmanager

1.191.1. RHBA-2009:1196: bug-fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1196

Updated rgmanager packages that fix a bug are now available.

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

This update applies the following bug fix:

- An issue that causes migrated virtual machines to restart after a cluster configuration update has been fixed.

Red Hat Resource Group Manager users are advised to upgrade to these updated packages, which address this issues.

1.191.2. RHBA-2009:0415: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0415

Updated rgmanager packages that fix three bugs are now available.

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

This update applies the following bug fixes:

- The SAP resource agents included in the rpmanager package shipped with Red Hat Enterprise Linux 5.3 were outdated. This update includes the most recent SAP resource agents and, consequently, improves SAP failover support.

- Exclusive service prioritization, whereby a high-priority exclusive service can take the place of a low-priority exclusive service, is now supported when central_processing is enabled. Note: this function does not work with virtual machines.
- An issue that causes virtual machines to restart after a configuration update has been fixed.

Red Hat Resource Group Manager users are advised to upgrade to these updated packages, which address these issues.

1.191.3. RHSA-2009:1339: Low security, bug fix, and enhancement update

An updated rgmanager package that fixes multiple security issues, various bugs, and adds enhancements is now available for Red Hat Enterprise Linux 5.

This update has been rated as having low security impact by the Red Hat Security Response Team.

The rgmanager package contains the Red Hat Resource Group Manager, which provides high availability for critical server applications in the event of system downtime.

Multiple insecure temporary file use flaws were discovered in rgmanager and various resource scripts run by rgmanager. A local attacker could use these flaws to overwrite an arbitrary file writable by the rgmanager process (i.e. user root) with the output of rgmanager or a resource agent via a symbolic link attack. (CVE-2008-6552)

This update also fixes the following bugs:

- clulog now accepts '-' as the first character in messages.
- if expire_time is 0, max_restarts is no longer ignored.
- the SAP resource agents included in the rgmanager package shipped with Red Hat Enterprise Linux 5.3 were outdated. This update includes the most recent SAP resource agents and, consequently, improves SAP failover support.
- empty PID files no longer cause resource start failures.
- recovery policy of type 'restart' now works properly when using a resource based on ra-skelet.sh.
- samba.sh has been updated to kill the PID listed in the proper PID file.
- handling of the '-F' option has been improved to fix issues causing rgmanager to crash if no members of a restricted failover domain were online.
- the number of simultaneous status checks can now be limited to prevent load spikes.
- forking and cloning during status checks has been optimized to reduce load spikes.
- rg_test no longer hangs when run with large cluster configuration files.
- when rgmanager is used with a restricted failover domain it will no longer occasionally segfault when some nodes are offline during a failover event.
- virtual machine guests no longer restart after a cluster.conf update.
- nfsclient.sh no longer leaves temporary files after running.
- extra checks from the Oracle agents have been removed.
- vm.sh now uses libvirt.
- users can now define an explicit service processing order when central_processing is enabled.

- virtual machine guests can no longer start on 2 nodes at the same time.
- in some cases a successfully migrated virtual machine guest could restart when the cluster.conf file was updated.
- incorrect reporting of a service being started when it was not started has been addressed.

As well, this update adds the following enhancements:

- a startup_wait option has been added to the MySQL resource agent.
- services can now be prioritized.
- rgmanager now checks to see if it has been killed by the OOM killer and if so, reboots the node.

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

1.192. rhn-client-tools

1.192.1. RHBA-2009:1354: bug fix and enhancement update

Updated rhn-client-tools packages that fix several bugs and add enhancements are now available.

Red Hat Network Client Tools provide programs and libraries that allow your system to receive software updates from the Red Hat Network (RHN).

These updated packages fix the following bugs and add the following enhancements:

- when selecting certificates, rhn_register created backup copies of the original cert each time a wrong cert is choose. (BZ#250312)
- when scheduling specific errata from the satellite or hosted Web user interface (WebUI), said errata did not get installed during rhn_check due to missing VREA as it took into account only the name. (BZ#464827)
- when rhn_check processed the action names, the sanity check was fragile for different locales (BZ#467139)
- running rhn_register on a xen guest caused mmap errors. (BZ#476797)
- rhn_check, while processing errata scheduled actions, installed extra 32-bit packages as it was ignoring the package architecture. (BZ#476894)
- rhn-client-tools should now depend on version 2.2.7 or newer of rhnlib. (BZ#487754)
- the --contactinfo option has been deprecated from the rhnreg_ks utility. (BZ#204449)
- parsing te_IN locale strings in the registration Graphical User Interface (GUI) caused a TypeError. (BZ#227638)
- firstboot registration logic was unaware of whether the system is already registered. (BZ#445881)
- when registration failed in the entitlement page, it should now be able to handle newer entitlement numbers. (BZ#454005)
- a typo ("receives" should be "receive") in the registration text user-interface (TUI) was corrected. (BZ#466718)

- the registration TUI should now be able to choose the cert if available in the default location automatically. If not it should prompt users to choose the cert. (BZ#471928)
- an option to not include network information while registration probes for hardware info is now provided. A new config option called sendNetwork has been added and is turned on by default. (BZ#479706)
- when haldaemon or messagebus are not running, hardware refresh should warn users that the daemon is not running instead of a generic dmi error. (BZ#491258)
- registration should not look for cert when using the insecure http protocol. The certificate should only matter when using the secure, https, protocol. (BZ#494928)
- rhn_register should now be able to identify kvm guests by sending the uuid and virt type to the server through smbios data. The kvm guests will be identified as kvm/qemu upon successfully registration. (BZ#495615)

All Red Hat Network users are advised to install this updated package which addresses these issues.

1.193. rhnlib

1.193.1. RHBA-2009:1353: bug fix and enhancement update

An updated rhnlib package that fixes various bugs and adds two enhancements is now available.

rhnlib is a collection of Python modules used by the Red Hat Network (RHN) software.

This updated package addresses the following bugs:

- when redirected to the content provider for packages, rhn client would not correctly register changes in protocol, which would result in a TypeError. (BZ#489920)
- when attempting to download multiple packages, only the first redirect URL would be stored, so not all packages pulled down would be correct. Changes in protocol and URLs are now tracked and redirecting should work as expected. (BZ#489921)
- when a package could not be found on the content delivery network, rhnlib would make an incorrect request to the original host, and use this URL for subsequent attempts to locate the package. rhn client now requests a fresh redirect when a package cannot be located on the network. (BZ#492638)
- if an attempt to open a file in /tmp failed, the SmartIO.py module would enter a loop and make multiple attempts to open the same file. If these all failed, the module would exit with an error. The module provided in this updated package instead uses mkstemp to create a file with a unique filename. This has a greater chance of success and uses system resources more efficiently. (BZ#499858)

This package also adds the following enhancements:

- rhnlib has been enhanced and should now be able to handle any redirect requests sent down by Red Hat Network servers. (BZ#484245)
- users were constrained to use the /tmp directory on the server's file system to store temporary transport files for transfer to the clients, and required space on client machines where the temporary transport files could be stored during installation. The version of rhnlib included with this advisory allows end-users to define their own temporary directory in which to spool temporary transport files.(BZ#499860)

All Red Hat Network users are advised to install this package which fixes these bugs and adds these enhancements

1.194. rhnsd

1.194.1. RHBA-2009:1356: bug fix update

An updated rhnsd package that fixes several bugs is now available.

rhnsd runs periodically to access a Red Hat Network server for software updates.

This updated package applies fixes for the following bugs:

- the rhnsd init script returned incorrect error codes and sometimes prevented correct status command calls. The init script has been updated so that it returns appropriate error messages, and the status command call error no longer presents. (BZ#243699)
- if a user's system was not registered on the Red Hat Network, the rhnsd postuninstall script would fail when attempting to upgrade from Red Hat Enterprise Linux 5.3 to Red Hat Enterprise Linux 5.4. As a result, the rhnsd update would fail. This updated package contains a workaround. To update the rhnsd package correctly, first uninstall the old version of rhnsd, and then install the new version. The postuninstall script will then work as expected.(BZ#503719)

Users are advised to upgrade to this updated rhnsd package, which resolves these issues.

1.195. rpm

1.195.1. RHBA-2009:1371: bug fix update

Updated rpm packages that resolve several issues are now available.

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

These updated rpm packages provide fixes for the following bugs:

- on 64-bit multilib systems, verifying all packages on the system led to a large number of files being listed which only differed in timestamp values. With this update, timestamp differences on multilib systems are now filtered so that verifying all packages (using the "rpm -Va" command) on both 32-bit and 64-bit systems results in relevant and useful information for system administrators. (BZ#426672 , BZ#472151)
- verification using the "--root [directory]" option could give false warnings on file ownership due to using the system's user and group database instead of the alternate root. RPM now performs verification using actual chrooted environment to ensure the correct user database is used. (BZ#434150)
- in some upgrade scenarios YUM would trigger a massive memory fragmentation in librpm, causing it to use immoderate amounts of memory. RPM now uses a better allocation algorithm to avoid excessive fragmentation. In addition, a separate flawed algorithm caused initial installation to take much longer than it should have. These fixes result in a better-performing RPM overall. (BZ#435475)
- the "rpmbuild" utility silently applied patches that no longer exactly match the source code, which could cause packaging of unwanted backup files or even result in subtle bugs in the software itself. An opt-in mechanism to enable a stricter mode of patching on a per-spec basis has been introduced to help packagers notice these cases early in the package-building process. (BZ#471005)
- on 64-bit multilib systems, RPM permitted installation of packages for incompatible architectures. RPM now validates package architecture compatibility on all platforms. (BZ#472065)
- an extra "/" character in source file paths could have caused RPM version 4.4.2.3 to abort builds on packages that were previously able to be built during the debug-information extraction stage. This update reverts the error to a warning to let such packages continue to build. (BZ#482903)

- RPM incorrectly calculated the fingerprint of some GPG public keys, causing false "key not present" errors on package signature-checking. This update includes a fix to correct the fingerprint calculation in these cases. (BZ#493777)
- recent RPM versions could fail to verify a valid RSA signature on a package due to different padding behavior of the low-level cryptography library now used. RPM now performs the additional zero-padding itself when necessary, thus allowing RSA signatures to be correctly verified. (BZ#502791)
- RPM output an invalid Japanese error message when run in a Japanese locale. The error message translation has been corrected. (BZ#387321)

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

1.196. rsh

1.196.1. RHBA-2009:0423: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0423

Updated rsh packages that resolve several issues are now available.

The rsh-server package contains programs which allow users to run commands on remote machines, log in to other machines, copy files between machines (rsh, rlogin and rcp), and provides an alternate method of executing remote commands (rexec). All of these programs are run by xinetd and can be configured through the Pluggable Authentication Modules (PAM) system, and through configuration files in the /etc/xinetd.d/ directory.

These updated rsh packages provide fixes for the following bugs:

- rsh did not set any of the environment variables listed in the /etc/security/pam_env.conf configuration file, and thus rsh users did not have access to that environment. With this update, rsh correctly reads and sets the environment variables listed in /etc/security/pam_env.conf, thus resolving the issue.
- the rexec(1) man page stated that the maximum length of the username on the remote system was restricted to 16 characters. Internally, however, rexec limited the maximum username length to 14 characters. rexec's maximum username length has been increased to 16 characters, which corresponds to the value given in the manual page, and which resolves the issue.
- when copying data to a full NFS directory, rcp failed silently and did not report an error, which led to silent data loss. With this update, rcp does report an error under this condition.

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

1.197. rt61pci-firmware

1.197.1. RHEA-2009:1255: enhancement update

An updated rt61pci-firmware package to support the rt61pci driver is now available.

Previously, due to a packaging error, users of Red Hat Enterprise Linux 5 on IBM S/390 systems received the rt61pci firmware package, even though it did not apply to their architecture. With the packaging error

corrected, Red Hat will continue to ship this package for 32-bit and 64-bit AMD and Intel platforms and for IBM POWER platforms, but not for IBM S/390. (BZ#488286)

1.198. rt73usb-firmware

1.198.1. RHEA-2009:1254: enhancement update

An updated rt73usb-firmware package that addresses a packaging issue is now available.

The rt73usb-firmware package contains the firmware required by the rt73usb driver in the kernel

The rt73usb driver is not included in the IBM S/390 and IBM System z kernels. Previously, however, rt73usb-firmware — an architecture-independent (noarch) package containing firmware required by the rt73usb driver — was automatically but unnecessarily included in the IBM S/390 and IBM System z distributions. For this update, the rt73usb-firmware package spec file was edited to include a 'ExcludeArch: s390 s390x' line. Consequently, although rt73usb-firmware is still a noarch package, it is no longer shipped with the IBM S/390 and IBM System z distributions.

1.199. ruby

1.199.1. RHSA-2009:1140: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1140

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

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

A flaw was found in the way the Ruby POP module processed certain APOP authentication requests. By sending certain responses when the Ruby APOP module attempted to authenticate using APOP against a POP server, a remote attacker could, potentially, acquire certain portions of a user's authentication credentials. (CVE-2007-1558)

It was discovered that Ruby did not properly check the return value when verifying X.509 certificates. This could, potentially, allow a remote attacker to present an invalid X.509 certificate, and have Ruby treat it as valid. (CVE-2009-0642)

A flaw was found in the way Ruby converted BigDecimal objects to Float numbers. If an attacker were able to provide certain input for the BigDecimal object converter, they could crash an application using this class. (CVE-2009-1904)

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

1.200. s390utils

1.200.1. RHBA-2009:1311: bug fix and enhancement update

An updated s390utils package that fixes multiple bugs and adds various enhancements is now available.

The s390utils package contains utilities related to Linux for the IBM S/390 architecture.

This update fixes these bugs:

- the dasdfmt tool prevented devices with record 0 set in the Define Extent CCW from being formatted, unless the channel program had initially changed the RO. This differed from the expected functionality. The tool has been updated to allow ECKD DASD devices that do not contain a default record 0 to be formatted. (BZ#474157)
- the /etc/profile.d/s390x.chs profile script was causing tcsh -e scripts to fail because the /sbin/consoletype was returning a non-zero value. The profile script has now been updated to supply a stdout argument that forces consoletype to return 0 in all cases. (BZ#505283)
- the ziomon tool contained an unsupported upstream patch from the blkiomon package. This resulted in the tool aborting when blkiomon was called by ziomon. The ziomon utility is now updated to use the new blkiomon_stat layout implemented by IBM. (BZ#506966)
- the lsluns tool was incorrectly displaying encrypted disks as unencrypted because the encryption check was performed on the 0x8 bit instead of the 0x80 bit. The lsluns tool now correctly displays the encryption status of the selected disk. (BZ#510032)

And adds these enhancements:

- the zipl tool prevented customers using a menu configuration file from disabling the automenu unless the -x option was specified. This caused confusion when using the tool, and forced customers to specify an extra option when using the utility. Customers are now able to specify the defaultmenu option, which displays the menu specified in the menu configuration file and disables the automenu. (BZ#486444)
- with this release, s390utils has been re-based from version 1.8.0 to upstream version 1.8.1. This re-base adds a range of new features, including the iucvterm tool and the zipl tool. Version 1.8.1 also addresses numerous bugs, including BZ#506966 . For details regarding these and other changes see the "Release History" section of the s390utils README file in /usr/share/doc/s390utils-1.8.1/. (BZ#477189)

S390 users should install this updated package which addresses these issues and adds these enhancements.

1.201. samba

1.201.1. RHBA-2009:1150: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1150

Updated samba packages that fix several bugs are now available.

Samba is a suite of programs used by machines to share files, printers, and other information.

These updated samba packages provide fixes for the following bugs:

- due to the method in which the Microsoft® Excel program saves files, in certain corner cases the access control list (ACL) inheritance rules could have been interpreted in the wrong order, and the owner of a file

saved by Excel could have ended up losing access to that file. These updated packages include an adjusted fix for this problem which fixes the ACL inheritance so that saving an Excel file does not cause the owner to change. (BZ#501513)

- a user who did not own a directory on a Red Hat Enterprise Linux 5 machine accessed via Samba was also unable to write to that directory when its permissions were set to 733. The user should have been able to both write to and enter (but not list the contents of) a directory with such a permission mode. With this update, users are once again able to write to directories over Samba when they possess the appropriate permissions, thus resolving this issue. (BZ#501514)

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

1.201.2. RHBA-2009:1416: bug fix update

Updated samba packages that resolve several issues are now available.

Samba is a suite of programs used by machines to share files, printers, and other utilities.

This update upgrades Samba to upstream version 3.0.33, which contains a number of bug fixes and enhancements over the previous version.

Notably, these updated samba packages provide fixes for the following bugs:

- due to the method in which the Microsoft Excel program saves files, in certain corner cases the access control list (ACL) inheritance rules could have been interpreted in the wrong order, and the owner of a file saved by Excel could have ended up losing access to that file. These updated packages include an adjusted fix for this problem which fixes the ACL inheritance so that saving an Excel file does not cause the owner to change. (BZ#481046)

- using smbclient to write files to a directory to which the user had permissions sufficient to write but not read resulted, incorrectly, in an "access denied" error. With these updated packages, smbclient correctly allows this operation. (BZ#497156)

- the "mount.cifs" utility reported an incorrect exit status upon exit. (BZ#465979)

- the VFS Recycle module's "touch" option did not work properly for non-administrator users. (BZ#470897)

- the pdbedit(8) man page incorrectly reported the existence of an invalid option. (BZ#457381)

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

1.202. sblim

1.202.1. RHBA-2009:1267: bug fix update

Updated sblim packages that fix a bug are now available.

SBLIM stands for Standards-Based Linux Instrumentation for Manageability. It consists of a set of standards-based, Web-Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.

These updated sblim packages provide fixes for the following bugs and add the following enhancement:

- when the sblim-cmpi-dhcp package is installed, it modifies the files under /var/lib/Pegasus owned by the

tog-pegasus package. Previously, when sblim was installed in the course of an "everything" installation of Red Hat Enterprise Linux 5 on the PowerPC architecture, the modifications that sblim made in the /var/lib/Pegasus directory prevented the post-install scriptlet from completing the provider-register commands. In turn, this would prevent installation of Red Hat Enterprise Linux 5 from completing. The provider-register commands are no longer provided in the post-install scriptlet, therefore avoiding this situation and allowing installation of the operating system to complete normally. Users of SBLIM who need to register provider modules for tog-pegasus should register these modules manually -- refer to the Red Hat Enterprise Linux 5.4 Technical Notes for instructions. (BZ#512123)

- the provider in the sblim-cmpi-network subpackage executes /sbin/ifconfig to generate localized output. In the section of the code that generates wbemcli output for IPv4 addresses, the language for ifconfig was not identified, with the result that no output was generated at all when the LANG= environment was set to anything other than en_US. IPv4Address, IPv6Address, and SubnetMask were then all reported as "NULL". The language passed to ifconfig is now specified as en_US, so that meaningful output is returned, regardless of the language of the environment. (BZ#458118)
- the spec file for the sblim package was originally written for use with an earlier version of the GNU Compiler Collection (GCC). Attempts to build the sblim package from source using more recent versions of the GCC would therefore fail. The spec file is now updated so that it works with current versions of the GCC. (BZ#496999)
- the sblim packages now include new CIM-based instrumentation to configure DHCP servers. This instrumentation is packaged in sblim-wbemsmt-dhcp. (BZ#442777)

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

1.203. scim-bridge

1.203.1. RHBA-2009:0426: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0426

Updated scim-bridge packages that resolve a memory leak are now available.

SCIM Bridge is a C implementation of a GTK+ IM module for SCIM.

These updated scim-bridge packages fix a memory leak in scim-bridge related to the D-Bus message header.

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

1.204. selinux-policy

1.204.1. RHBA-2009:1242

The selinux-policy packages contain the rules that govern how confined processes run on the system.

The selinux-policy package has been updated, providing the following enhanced policy changes for SELinux:

- samba previously could not directly change a user's password via the passwd program.(BZ#429726)
- newer versions of the system RAID utilities were previously blocked from logging properly when running SELinux in Enforcing mode.(BZ#475562)
- the **postgrey** utility can now operate properly over a network socket.(BZ#479819)
- the installation of RPM files on the PowerPC architecture is no longer blocked.(BZ#480163)
- **NetworkManager** is now permitted to discover the priority of related processes.(BZ#480943)
- **procmail** is now permitted to operate with and call the **spamassassin** application.(BZ#481387)
- **hald** is now permitted to send messages via **dbus** bi-directionally.(BZ#481628)
- system signals are now permitted to be sent properly to the **automount** daemon.(BZ#481706)
- the **samba_enable_home_dirs** Boolean now allows access to hidden files in home directories.(BZ#484146)
- the default context for files related to the **sysstat** package have been corrected.(BZ#485078)
- **procmail** now permitted to execute anti-spam daemons.(BZ#485107)
- **samba** can now access **public_html** directories.(BZ#485111)
- the default label for the sa-learn binary used by **spamassassin** has been modified to the correct value.(BZ#486187)
- the building of policies for a low-privileged user is now permitted when using **selinux-policy-strict**.(BZ#486354)
- library files for the **MATLAB** environment are now correctly labelled. (BZ#486965)
- **samba** is now permitted to properly rotate log files.(BZ#487021)
- **dbus** is now permitted to read parts of the proc file system for its system messages.(BZ#489899)
- the name service cache daemon no longer unexpectedly restarts due to a lack of search permissions.(BZ#490024)
- the **proc** file system is now correctly labelled by the restorecon command.(BZ#492567)
- search privileges are now granted to **dnsmasq** (when **dnsmasq** is launched using **libvirt**).(BZ#496867)
- **Openswan** can now correctly access the Network Security Services libraries.(BZ#497168)
- **autofs** now restarts normally when active mounts exist.(BZ#497273)
- the **amanda** backup utility can now send all required signals to the system.(BZ#498596)
- proper operation of xen guests via the **virsh** utility is now permitted.(BZ#499249)
- HP printers now properly scan and operate over a network socket.(BZ#499691, BZ#504398)
- **spamd** now restarts properly when a HUP signal is issued.(BZ#499701)
- the **clamav-milter** binary was previously labeled with an incorrect context, preventing clamd from running in the correct domain.(BZ#500392)

- **setkey_t** subjects can now read required files, such as those created by initscripts.(BZ#500395)
- previously, a SELinux-related file in the selinux-policy-minimum package was unable to be properly installed.(BZ#502182)
- the state of the **qemu_full_network=1** Boolean is now enabled by default.(BZ#504238)
- TUN/TAP drivers are now given full network socket access.(BZ#504738)
- the required TCP port is added for the Cyrus IMAP Aggregator (mupdate).(BZ#504805)
- Host-Guest File Systems under **VMware** can now be properly mounted.(BZ#504872)
- **iscsi-initiator** can now run with full capability without causing denials. (BZ#506057)
- previously, **procmail** application may have caused an fsetid denial. (BZ#507712)
- the connection created by the **dblink_connect** functionality of PostgreSQL is no longer blocked. (BZ#508348)
- the **Winbind** subsystem can now modify Kerberos related configuration files. (BZ#509174)
- the attributes of the **lsmod** command have been updated allowing lsmod to properly query the state of kernel modules. 510188
- the allow_unconfined_mmap_low boolean setting was not properly applied to the unconfined_t domain - even when turned off, unconfined_t processes were still allowed to map low memory pages. Note: Refer to Knowledgebase article DOC-18042 for more information about the handling of the low memory pages mapping restriction on systems with SELinux. (BZ#511143)
- This update allows objects and processes running in the **ipsec_t** domain to read files labeled as **initrc_exec_t**. This is required for the **/etc/rc.d/init.d/ipsec** file to be launched properly. (BZ#511359)
- the automount subsystem can now use the winbind mechanism as specified in **/etc/nsswitch.conf**. (BZ#511927)
- all files in the **/var/vdsm** directory have the same SELinux file contexts. (BZ#512301, BZ#513208)

Additionally, minor typographical errors have been fixed in the httpd_selinux, kerberos_selinux, nfs_selinux and rsync_selinux man pages. (BZ#477123)

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

1.205. setroubleshoot

1.205.1. RHBA-2009:1080: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1080

Updated setroubleshoot packages that resolve an issue are now available.

The setroubleshoot packages provide tools to help diagnose SELinux problems. When AVC messages

occur, an alert is generated that gives information about the problem, and how to create a resolution.

These updated setroubleshoot packages fix the following bug:

- shutting down the system caused setroubleshoot to report that the connection had failed. This was caused by an inoptimal ordering in the system shutdown scripts wherein the D-Bus system message bus was shut down before setroubleshoot, which resulted in connection failure messages. The relative order in which setroubleshoot and D-Bus are shut down has been switched, and setroubleshoot no longer reports failure at shutdown time. (BZ#449228)

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

1.206. setup

1.206.1. RHBA-2009:0484: bug fix and enhancement update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0484

An updated setup package that fixes several bugs and adds various enhancements is now available.

The setup package contains a set of important system configuration and setup files, such as passwd, group, and profile.

This updated setup package fixes the following two inconsistencies between the bash and the csh and tcsh profile scripts:

- in order to match the bash shell's default behavior and provide consistency across shells, csh files in the /etc/profile.d/ directory are not read when csh is loaded as a non-login shell.

- when using the csh or tcsh shell, the user's umask is now set exactly the same as it is for the bash shell. If a process owned by a user creates a file, the UID number of the user is 100 or greater, and the username and group name match, then the umask of the process will be set to "002". Otherwise, the umask will be set to "022".

In addition, this updated package provides the following enhancements:

- this updated setup package reserves the new "tss" User ID and Group ID, and the userid (UID) and groupid (GID) numbers (59:59), which should prevent accidental usage of that UID/GID pair by other packages and administrators. TrouSerS is an implementation of the Trusted Computing Group's Software Stack (TSS) specification.

- this updated setup package reserves the new "puppet" user ID and group ID, and the userid (UID) and groupid (GID) numbers (52:52), which should prevent accidental usage of that UID/GID pair by other packages and administrators. Puppet is an automated system administration engine that performs tasks such as adding users, installing packages, and updating server configurations based on a centralized specification language.

- this updated setup package reserves the new "pkiuser" user ID and group ID, and the userid (UID) and groupid (GID) numbers (17:17), which should prevent accidental usage of that UID/GID pair by other packages and administrators. The "pkiuser" user and group IDs are used in subsystems associated with the Red Hat Certificate System.

- this updated setup package reserves the new "vdsm" user ID and "kvm" group ID, and the userid (UID) and groupid (GID) numbers (36:36), which should prevent accidental usage of that UID/GID pair by other packages and administrators. VDSM service manages a single SolidICE node (VDS). It serves as a proxy for Virtual Machine creation, management, statistics, and log collection.
- this updated setup package reserves the new "oprofile" user ID and group ID, and the userid (UID) and groupid (GID) numbers (16:16), which should prevent accidental usage of that UID/GID pair by other packages and administrators. The "oprofile" user and group IDs are used by the OProfile program, a low-overhead, system-wide profiler capable of running transparently in the background.

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

1.207. sg3_utils

1.207.1. RHBA-2009:1357: bug fix and enhancement update

Updated sg3_utils packages that fix several bugs and add an enhancement are now available.

The sg3_utils package contains a collection of tools for SCSI devices that use the Linux SCSI generic (sg) interface. It includes utilities to copy data based on "dd" syntax and semantics (the sg_dd, sgp_dd and sgm_dd commands), check INQUIRY data and associated pages (sg_inq), check mode and log pages (sg_modes and sg_logs), spin disks up and/or down (sg_start) and perform self-tests (sg_senddiag), along well as various other utilities.

These updated sg3_utils packages provide the following enhancement:

- for Red Hat Enterprise Linux 5.4 a new shell script, "rescan-scsi-bus.sh", has been added to the sg3_utils package. This script utilizes the capabilities of the Linux kernel to add and remove SCSI devices without the need to reboot the machine or reload a kernel module. (BZ#507379)

  This script should be considered a Technology Preview for Red Hat Enterprise Linux 5.4.

Warning

the rescan-scsi-bus.sh script can remove storage devices from the system as well as add them. Before issuing any command that may cause device removal from the operating system, close all users of the device; unmount any file systems mounting the device; and remove the device from any dm, md, LVM, multipath or RAID setups using it. If you intend, therefore, to add or remove devices from a bus while i/o is on-going, perform these operations on one device at a time and check the results as each step is completed. Do not perform a scan that adds and removes devices at the same time. See the Online Storage Reconfiguration Guide for a complete overview of this topic. (BZ#467201)

Note

"sd" device names are not persistent and may change when devices are removed or added. Use WWIDs or disk metadata to reliably identify devices.

In addition, these updated sg3_utils packages provide fixes for the following bugs:

- the "sg_map26" command was unable to correctly map the device names for greater than 32 tape drives on a single system. This has been fixed so that it can correctly map 32 or more tape drives. (BZ#468040)
- the "sg_map26" command's usage information contained an incorrect statement regarding what function the '--verbose' ('-v') flag performed. The usage information for this command has been clarified. (BZ#431190)
- the "sg_test_rwbuf" command's usage information showed the '--verbose' ('-v') description twice, and omitted the line describing the '--version' option. This has been fixed in these updated packages. (BZ#431193)
- the "sginfo" command's information page omitted a description for the '-v' option. (BZ#433614)
- the "sg_wr_mode" command's information page contained the option '--hex', which is non-existent, instead of '--help'. (BZ#433773)
- due to an option-handling error, the "sg_get_config" command's '--brief' and '-b' options, which show undecoded feature names, presented differing output. (BZ#433779)
- the "sg_ses" command's usage information contained a typo: the option is actually '--byte1' instead of simply '--byte'. (BZ#435100)
- the "sg_read_long" command sometimes exited with an incorrect exit code. This has been fixed in these updated packages. (BZ#435275)
- the "sg_persist" command's usage information incorrectly contained a reference to the '--prout-sark' option instead of, correctly, '--param-sark'. (BZ#435677)
- the sg_wr_mode(8) man page contained, in the "EXAMPLES" section, examples that used incorrect options with the "sg_modes" comamnd. These command string examples have been corrected. (BZ#437147)

Users are advised to upgrade to these updated sg3_utils packages, which resolve these issues and add this enhancement.

1.208. sos

1.208.1. RHBA-2009:0461: bug fix and enhancement update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0461

An updated sos package that fixes several bugs and adds various enhancements is now available.

sosreport is a tool that collects information about a system, such as which kernel is running, what drivers are loaded, and scans various configuration files for common services. It also performs some simple diagnostics against known problematic patterns.

This updated sos package provides fixes for the following bugs:

- sosreport became unresponsive in a virtualized environment if the xend daemon had not been started. (BZ#497506)

1.208.2. RHBA-2009:1418: bugfix and enhancement update

Sos is a set of tools that gathers information about system hardware and configuration. The information can then be used for diagnostic purposes and debugging. Sos is commonly used to help support technicians and developers.

This updated package provides the following bug fixes and enhancements.

* The French translation of **sos** would prompt the user **`Voulez vous continuer (y/n)?`** but would ignore **`y`** as an answer and would only accept **`o`** or **`n`**. The prompt has now been corrected to reflect the actual options. (BZ#469365)

* Previously, **sos** could handle only default, conventional python paths. When run on systems with unconventional python paths, **sos** would crash. **Sosreport** is now tolerant of unconventional python paths and will not crash when it encounters them. (BZ#480302)

* For security reasons, **sos** sanitizes passwords that would otherwise appear in its report, including the shared secret (**`bindpw`**) from **`/etc/ldap.conf`**. Previously, if **`/etc/openldap/ldap.conf`** were symbolically linked to **`/etc/ldap.conf`**, **sos** would sanitize the **`bindpw`** in ldap.conf itself. Now, **sos** only sanitises the **`bindpw`** that is included in its report. (BZ#475190)

* Although **sos** is designed to run unattended if required to do so, recent versions still prompted users for input during diagnose method tests if the test found any problem. This prompt meant that **sos** was unable to run unattended. Furthermore, when it did not receive a reply to the prompt, **sos** would crash. **Sosreport** now automatically chooses the option to continue instead of prompting the user whether to continue or not, and can therefore run unattended. (BZ#475991)

* Previously, faulty logic in **rh-upload-core** prevented it from uploading a core if the quiet flag were not set. Additionally, the destination directory was incorrectly specified as **`dropbox.redhat.com`**. Now, **`rh-upload-core`** can upload a core regardless of the status of the quiet flag, and correctly sends the core to **`dropbox.redhat.com/incoming`**. (BZ#477042)

* When used with the Xen plugin, **sos** would stop responding due to flaws in the code of the plugin. In particular, a misnamed function would result in the plugin attempting to collect data from a Xen kernel when **xend** was not running. With these flaws corrected, the Xen plugin now works correctly and does not cause **sos** to stop responding. (BZ#490186)

* **Sos** archives its findings in a tar.bz2 file. However, neither **tar** nor **bzip2** were listed as requirements in the *sos* package. Therefore, on minimal installations that included neither of these tools, **sos** would produce an empty tar.bz2 file. **Sos** now requires both these tools, which enable it to create its report.(BZ#503536)

* The Xen plugin for **sos** was looking for the presence of fully virtualized guests by searching for **`int-xen`** in **`/proc/acpi/dsdt`**. Due to changes in how the Xen hypervisor is implemented in Red Hat Enterprise Linux, this approach does not work with updates newer than Red Hat Enterprise Linux 5.1. The Xen plugin now searches for **`xen`** in **`/proc/acpi/dsdt`** instead and can therefore identify fully virtualized guests. (BZ#460788)

* The **sos** cluster plugin did not account for situations where the system locale may be set to something other than US English. On a system with a different locale, the plugin could not start chkconfig and therefore did not work. The cluster plugin now starts chkconfig with **`LC_ALL=C`** set, and works as intended. (BZ#462824)

* The **sos** RHN plugin obtained information from **`/home/nocpulse/`** and **`/opt/notifications`**. However, RHN monitoring is now logged in **`/var/log/nocpulse/`** and **`/var/log/notification/`** instead. The plugin continues to search for logs in **`/home/nocpulse/`** and **`/opt/notifications/`** in order to preserve backward compatibility, but now searches for logs in **`/var/log/nocpulse/`** and **`/var/log/notification/`** too. (BZ#480786)

* Previously, **sos** imported data from **snack**, but did not use this data. However, in order to support this import, **sos** required three packages: *snack*, *libnewt*, and *libslang*. By avoiding the import, the packages are not otherwise required by **sos**, and if they are not required by any other component, they need not be

installed. Avoiding unneccessary packages simplifies support and minimizes the space required to install Red Hat Enterprise Linux. (BZ#497840)

* As part of its report, **sos** lists the packages installed on the system. Previously, **sos** stored these in the order that they were provided by the **`rpm -qa`** command. Now, **sos** sorts the packages into alphabetical order as it compiles its list. Listing the packages alphabetically makes it easier to find packages visually, and groups some related packages together. (BZ#498474)

* **Sos** now includes a batch mode, in which it does not ask any questions during its run. Batch mode is invoked with the **`--batch`** option. (BZ#501842)

* Previously, the **sos** plugin that collects **postfix** data was simply named **`mail.py`**. This name was too generic to be meaningful, and was not consistent with the naming of other plugins. The plugin is now named **`postfix.py`**, which better describes what data it collects. (BZ#464207)

* Previously, **sos** reports included the contents of **`/var/log/httpd`**. This could make the reports very long, sometimes over 300 MB. Because the information contained in **`/var/log/httpd`** is relevant to few troubleshooting cases, **sos** no longer obtains it. If necessary, the contents of **`/var/log/httpd`** can still be obtained by using the apache **sos** plugin. (BZ#433040)

* **Sos** now includes many new plugins to support the collection of data from a wider range of applications. The new plugins allow **sos** to gather information about:

- **kvm** (BZ#497206)
- **Directory Server** (BZ#461799)
- **dovecot** (BZ#464208)
- **netdump** (BZ#466819)
- **IPA** (BZ#466947)
- **anaconda** (BZ#472108)
- Smartcard-related details (BZ#497206)
- **sar** (BZ#469626)
- **snmp** configuration (BZ#472857)
- **kdump** configuration (BZ#4728558)
- **nscd** (BZ#487116)
- **tftp**-related details (BZ#487119)
- **oddjob**-related details (BZ#487308)
- **iscsi** (BZ#487466)
- **ntpdata** (BZ#487470)
- **tomcat5** (BZ#487474)
- **Auditd**-related information (BZ#487476)
- DHCP-related information (BZ#487477)
- **Red Hat Hardware Test Suite**-related information (BZ#487478)

- **udev**-related information (BZ#487480)
- PXE-related information (BZ#487481)
- **VMWare**-related information (BZ#487482)
- process accounting-related information (BZ#487483)
- **MySQL**-related information (BZ#487484)
- **MRG Messaging**-related information (BZ#487485)
- **MRG GRID**-related information (BZ#487488)
- **openssl**-related information (BZ#487628)
- **wvdial**- and **ppp**-related information (BZ#488412)

* **Sos** now includes information on a wider range of system parameters in its reports than it did previously. Newly collected details include:

- the contents of **`/var/log/pm/suspend.log`** (BZ#492072)
- **cron** jobs, including system and user jobs (BZ#487416)
- the default Java Runtime Environment (JRE) when multiple JREs are installed (BZ#503172)
- the results of **`ethtool -i`**, **`ethtool -k`**, and **`ethtool -S`** (BZ#469820)
- **logrotate** details (BZ#487434)
- the results of **`lspci -t`** (BZ#238778)
- state information of fibre channel devices (BZ#444839)
- the contents of **`custom.conf`** (BZ#450997)
- **dmesg** output (BZ#460140)
- the contents of **`/var/log/acpid`** (BZ#487113)
- various printing-related information, including global **`lpoptions`**, the **ppd** files used by assigned printers, and **`lpstat`** commands to see the printers in use and the URIs assigned to them (BZ#466923)

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

1.209. sqlite

1.209.1. RHBA-2009:0441: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0441

Updated sqlite packages that resolve an issue are now available.

SQLite is a C library that implements an SQL database engine.

These updated sqlite packages fix the following bug:

- using SQL's "explain" command caused the sqlite database to segmentation fault due to faulty opcode name auto-generation. A backported patch prevents this segmentation fault and causes the "explain" command to work as expected, thus resolving this issue.

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

1.210. squirrelmail

1.210.1. RHSA-2009:1066: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1066

An updated squirrelmail package that fixes multiple security issues is now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

SquirrelMail is a standards-based webmail package written in PHP.

A server-side code injection flaw was found in the SquirrelMail "map_yp_alias" function. If SquirrelMail was configured to retrieve a user's IMAP server address from a Network Information Service (NIS) server via the "map_yp_alias" function, an unauthenticated, remote attacker using a specially-crafted username could use this flaw to execute arbitrary code with the privileges of the web server. (CVE-2009-1579)

Multiple cross-site scripting (XSS) flaws were found in SquirrelMail. An attacker could construct a carefully crafted URL, which once visited by an unsuspecting user, could cause the user's web browser to execute malicious script in the context of the visited SquirrelMail web page. (CVE-2009-1578)

It was discovered that SquirrelMail did not properly sanitize Cascading Style Sheets (CSS) directives used in HTML mail. A remote attacker could send a specially-crafted email that could place mail content above SquirrelMail's controls, possibly allowing phishing and cross-site scripting attacks. (CVE-2009-1581)

Users of squirrelmail should upgrade to this updated package, which contains backported patches to correct these issues.

1.211. strace

1.211.1. RHBA-2009:0309: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0309

An updated strace package that fixes a bug is now available.

The strace program intercepts and records the system calls that are made and the signals that are received by processes.

This updated strace package fixes a bug which occurred when "strace -f" was used to trace a multithreaded program. strace selected threads to trace in an inoptimal manner, which could have caused certain threads to either run more slowly or to perpetually wait. With this update, strace selects threads to trace in a smarter manner, thus ensuring that no threads are left overlong in a waiting state, and therefore resolving the issue.

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

1.211.2. RHBA-2009:0017: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0017

Updated strace packages that fix one bug are now available.

The strace program intercepts and records the system calls that are made and the signals that are received by processes.

The following issue has been addressed:

- when a stopped process being examined by strace is killed, strace now reports the event correctly. The prime example is a SIGKILL being sent to a traced process.

Users of strace should upgrade to these updated packages, which resolves this bug.

1.211.3. RHBA-2009:1317: bug fix update

An strace update that fixes several bugs is now available.

The strace program intercepts and records system calls issued and received by a running process. Strace can print a record of each system call, its arguments and its return value.

With this update, strace is now upgraded to version 4.5.18. This applies several upstream bug fixes and enhancements, including:

- An erroneous file locking instruction caused strace to incorrectly decode fcntl64() system call parameters in 32-bit programs running on 64-bit systems. This release corrects the errant file locking instruction, ensuring that fcntl64() system call parameters are decoded correctly. (BZ#471169)

- A race condition made it possible for ptrace_do_wait() to prematurely conclude an exit report of a terminated process before the kill signal could set the proper exit code. Whenever this occurred, strace could leave out details of the kill signal in its exit report. This update applies a workaround that instructs strace to check SIGKILL queues before issuing an exit report. (BZ#472053)

- When strace was executed with the -f option on a multi-threaded process, it was possible for some threads in that process to stop. This could prevent the traced process from terminating. This was caused by a bug that prevented some threads in a traced multi-threaded process from receiving ample CPU time. This update provides functions for providing CPU time to threads in traced multi-threaded processes, along with instructions for resuming halted threads. (BZ#478419)

Users of strace should apply this update.

1.212. subversion

1.212. subversion

1.212.1. RHSA-2009:1203: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1203

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

This update has been rated as having important security impact by the Red Hat Security Response Team.

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.

Matt Lewis, of Google, reported multiple heap overflow flaws in Subversion (server and client) when parsing binary deltas. A malicious user with commit access to a server could use these flaws to cause a heap overflow on that server. A malicious server could use these flaws to cause a heap overflow on a client when it attempts to checkout or update. These heap overflows can result in a crash or, possibly, arbitrary code execution. (CVE-2009-2411)

All Subversion users should upgrade to these updated packages, which contain a backported patch to correct these issues. After installing the updated packages, the Subversion server must be restarted for the update to take effect: restart httpd if you are using mod_dav_svn, or restart svnserve if it is used.

1.213. sudo

1.213.1. RHSA-2009:0267: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0267

An updated sudo package to fix a security issue is now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root with logging.

A flaw was discovered in a way sudo handled group specifications in "run as" lists in the sudoers configuration file. If sudo configuration allowed a user to run commands as any user of some group and the user was also a member of that group, sudo incorrectly allowed them to run defined commands with the privileges of any system user. This gave the user unintended privileges. (CVE-2009-0034)

Users of sudo should update to this updated package, which contains a backported patch to resolve this issue.

1.213.2. RHBA-2009:0438: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0438

An updated sudo package that fixes one bug is now available.

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root with logging.

This updated sudo package fixes the following bug:

- sudo was unable to send email updates concerning sudo actions because "mailerflags" and "mailerpath" were not set. Sudo had to be recompiled with sendmail installed in the build environment to enable the auto-configuration system guess the right default values for "mailerflags" and "mailerpath". This update has compiled in default values for "mailerflags" and "mailerpath" and sudo is now able to send email about sudo actions after install.

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

1.214. system-config-cluster

1.214.1. RHBA-2009:1401: bug-fix and enhancement update

An updated system-config-cluster package that fixes bugs and adds enhancements is now available.

The system-config-cluster package contains a utility that allows management of cluster configuration in a graphical setting.

This update applies the following bug fixes:

- An issue with name fields in the LVM, Tomcat5 and PostGres resource agents has been fixed.
- A missing CMAN attribute is now included in the schema checker, thereby avoiding an error message.

Also, this update adds the following enhancements:

- Support for configuring subnet suffixes in the IP resource agent.
- An nfslock checkbox has been added to service management.
- Support for extended configuration settings is now available for SAP DB as well as SAP Instance.

Users should upgrade to this updated package, which resolves these issues and adds these enhancements.

1.215. system-config-date

1.215.1. RHBA-2009:0279: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0279

An updated system-config-date package that fixes a bug when run by firstboot is now available.

system-config-date is a graphical interface for changing the system date and time, configuring the system time zone, and setting up the NTP daemon to synchronize the time of the system with an NTP time server.

When run as part of firstboot, system-config-date erroneously deleted some widgets instead of hiding them. This caused "An error has occurred in the timezone module..." errors to present when trying to display the time-zone screen. With this update the widgets are, correctly, hidden and not removed, ensuring the time-zone screen displays as expected.

All users should upgrade to this updated package, which resolves this issue.

1.216. system-config-language

1.216.1. RHBA-2009:1074: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1074

An updated system-config-language package that fixes a bug in the locale-list is now available.

system-config-language is a graphical user interface that allows the user to change the default language of the system.

This updated package fixes the following bug:

- the locale-list used by system-config-language (located at /usr/share/system-config-language/locale-list) included latarcyrheb-sun16 as the default Romanian UTF-8 keymap. This keymap did not display the characters ș and ț (s and t with comma below) or ş and ţ (s and t with cedilla below) properly. With this update the locale-list's Romanian keymap defaults to Lat2-Terminus16, allowing for the correct display of these characters. (BZ#386741)

All users should upgrade to this updated package, which resolves this issue.

1.217. system-config-network

1.217.1. RHBA-2009:1352: bug fix and enhancement update

An updated system-config-network package that fixes two bugs and adds an enhancement is now available.

System-config-network is the user interface of the network configuration tool, supporting Ethernet, Wireless, TokenRing, ADSL, ISDN and PPP.

This updated package adds the following bug fixes and enhancement:

- previously, the textual user interface (TUI) version of system-config-network contained a reference to the "Primary DSN". This typo has now been corrected to "Primary DNS". (BZ#496307)
- previously, system-config-network did not set the MACADDR network parameter. The lack of this parameter made it impossible to enable layer 2 interfaces on IBM System z without further manual configuration. The MACADDR parameter has now been added to QETH dialogs and internal structures or system-config-network, enabling the configuration of layer 2 interfaces. (BZ#484289)
- previously, when system-config-network configured QETH interfaces in textual user interface (TUI) mode, it attempted to set ports whether the hardware existed or not. When the tool attempted to configure non-existent hardware, it would crash. Now, system-config-network tests whether hardware exists before configuring it. This allows users to configure QETH interfaces with the TUI tool without causing a crash. (BZ#507766)

All users are advised to upgrade to this updated package, which resolves these issues and adds this enhancement.

1.218. system-config-samba

1.218.1. RHBA-2009:1329: bug fix update

An updated system-config-samba package that fixes several bugs is now available.

The system-config-samba package provides a graphical user interface for creating, modifying, and deleting samba shares.

This update applies the following fixes from upstream:

- A bug prevented system-config-samba from honoring the custom 'username map' parameter in /etc/samba/smb.conf, overwriting it instead with /etc/samba/smbusers as a hard-wired path for Windows-to-Unix username mappings. As a result, attempts to access the samba service as a Windows user failed. This release applies an upstream patch that corrects this bug, ensuring that system-config-samba no longer ignores the 'username map' parameter. (BZ#460262)
- A bug caused system-config-samba to crash with a traceback error (instead of reporting the appropriate exit/error code) whenever system-config-samba encountered any unknown configuration options in /etc/samba/smb.conf. This updated version corrects the issue, ensuring that system-config-samba generates a proper error message regarding any unknown configuration options in /etc/samba/smb.conf. (BZ#460270)
- Whenever a Samba user did not explicitly set a Windows username, system-config-samba added a malformed line into the username map file. This malformed line prevented samba from building a user list. With this update, system-config-samba no longer adds the malformed line, allowing samba to build a user list even if a Samba user does not explicitly set a Windows username. (BZ#460271)
- After editing an existing user, a GUI bug locked the 'Unix Username' field of the 'Add user' window, preventing the creation of new users. This bug is now resolved, allowing the addition of new users after editing existing ones. (BZ#460291)

Users of system-config-samba are advised to upgrade to this update.

1.219. systemtap

1.219.1. RHSA-2009:0373: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0373

Updated systemtap packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

SystemTap is an instrumentation infrastructure for systems running version 2.6 of the Linux kernel. SystemTap scripts can collect system operations data, greatly simplifying information gathering. Collected data can then assist in performance measuring, functional testing, and performance and function problem diagnosis.

A race condition was discovered in SystemTap that could allow users in the stapusr group to elevate privileges to that of members of the stapdev group (and hence root), bypassing directory confinement restrictions and allowing them to insert arbitrary SystemTap kernel modules. (CVE-2009-0784)

Note: This issue was only exploitable if another SystemTap kernel module was placed in the "systemtap/" module directory for the currently running kernel.

Red Hat would like to thank Erik Sjölund for reporting this issue.

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

1.219.2. RHBA-2009:1313: bug fix and enhancement update

Updated **systemtap** packages that fix various bugs, enhance user-space probing, improve support for debuginfo-less operations and apply several other enhancements are now available.

SystemTap provides an instrumentation infrastructure for systems running the Linux 2.6 kernel. It allows users to write scripts that probe and trace system events for monitoring and profiling purposes. SystemTap's framework allows users to investigate and monitor a wide variety of wide variety of kernel functions, system calls, and other events that occur in both kernel-space and user-space.

With this update, SystemTap is now re-based on upstream version 0.9.7. This applies several enhancements and bug fixes, namely:

- On-file flight recording is now supported. This allows **stap** to run in the background and record huge trace log information on the disk, rather than just to memory. (BZ#438737)
- Kernel tracepoints are now supported for probing predefined kernel events without any debuginfo information. Tracepoints incur less overhead than kprobes, and context parameters are available with full type information. For a list of available, supported tracepoints, run the command **stap -L 'kernel.trace("*")'**. (BZ#475456 and BZ#498040)
- A SystemTap initscript is now included with this release, and is provided by the package **systemtap-initscript**. This initscript allows users to run SystemTap scripts as system services (in flight recorder mode) and control those scripts individually. For more information, refer to **/usr/share/doc/systemtap-initscript-<*version*>/README.initscript**. (BZ#474906 and BZ#481705)
- This update resolves a ref-count problem that prevented uprobes from properly disposing the uprobe_process struct on exec while there are outstanding uretprobe instances. In addition, a bug that caused utrace to incorrectly report events-in-progress to a recently-created engine is now fixed as well.

These fixes address several uretprobe bugs that could cause the system to hang in previous releases. (BZ#478711)

- SystemTap log rotation is now supported. With this, a running SystemTap script can switch to a different log file during on-file flight recording without stopping. Users can specify a time or log file size that triggers a log rotation, helping ensure that a SystemTap script never stops recording information. (BZ#481704)

- **stapprep.sh** is a script documented in the *SystemTap Beginner's Guide*, used to determine and download (when able) the kernel information packages needed to run SystemTap. This script is now included by default in the systemtap package as the command **stap-prep**. (BZ#485498)

- When **stap** passed a kill signal to its children, it was possible for that signal to be sent to all other processes in the same process group. This could include processes other than its children. This was because SystemTap used **system()** to manipulate process groups. With this update, SystemTap now uses **stap_system()** instead of **system()**; this allows **stap** to save the process ID of all its children, ensuring that **stap** only sends signals to its children. (BZ#494462)

- Probes that used **insn** probe points failed. While the upstream version of SystemTap fully supports the use of **insn** probe points, the kernel and utrace versions used by Red Hat Enterprise Linux 5 did not define the required macros **arch_has_single_step()** and **arch_has_block_step()**. With this release, SystemTap defines these macros during compile time whenever **insn** probe points are used. (BZ#498018)

- The **systemtap-testsuite** package contained test cases (**systemtap.base/bz10078.stp**, **buildko/two.stp**, and **buildok/thirty.stp**) that were incorrectly configured as "executable". Any test runs involving these cases failed unexpectedly. This release fixes the permissions for all test cases provided by the **systemtap-testsuite** package. (BZ#499657)

- The **context.stp** tapset now contains a definition for the **task_pt_regs()** macro, which is required to compile some types of SystemTap scripts on the PowerPC platform. (BZ#499688)

- Compiling any program that used static dynamic trace markers for the **STAP_PROBE** or **DTRACE_PROBE** macros on the PowerPC platform resulted in an error. This was caused by an incorrect **if/else** statement in the **sdt.h** headr file, did not define PowePC as required; as such, the **sdt.h** header file supplied an incorrect macro definition for **STAP_NOP**. With this update, **sdt.h** now provides the correct macro definition for **STAP_NOP** on the PowerPC platform. (BZ#501795)

- A bug in the implementation of kernel return probe trampolines made it possible for some stack tracebacks to go undetected. Whenever this occurred, the stack unwinder would not be executed, resulting in a garbled stack. With this release, the code for detecting the kernel return probe trampoline is now fixed, ensuring that all stack tracebacks are dealt with accordingly. In addition, this release also uses the kernel DWARF unwinder automatically in the event of stack tracebacks. (BZ#503225)

- A bug in **runtime/task_finder.c** made it possible for some processes to hold a semaphore while performing a memory map callback. Whenever this occurred, some tasks would become deadlocked if they were probed by user-space probes. This update fixes the bug, ensuring that memory map callbacks are safe and do not cause deadlocks. (BZ#504007)

SystemTap is no longer a technology preview, and now has production support. Red Hat recommendeds that users run scripts on development machines before deployment in production environments. Since SystemTap is an optional diagnostic tool, users can easily stop using it in the event of a problem. Options such as **-g** for Guru mode, and **-D*** allow users to disable several security checks. Scripts using these options may not be supported.

Red Hat plans to fix problems in SystemTap, or the Linux kernel, as they arise in connection with new scripts. In some cases, a fix may include extending the blacklist for known areas of the Linux kernel that are unsafe to probe. All scripts that use probes targeting blacklisted areas will need to be revised.

SystemTap users are advised to upgrade to this version.

1.220. tcl

1.220.1. RHBA-2009:0414: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0414

Updated tcl packages that resolve an issue are now available.

Tcl is a simple scripting language designed to be embedded into other applications. Tcl is designed to be used with Tk, a widget set.

These updated tcl packages fix a bug which resulted in "wrong ELF class: ELFCLASS32" error messages when attempting to run tcl scripts on a 64-bit multilib system where both the 32-bit and 64-bit packages dependent on tcl were installed.

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

1.221. tcp_wrappers

1.221.1. RHBA-2009:0453: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0453

Updated tcp_wrappers packages that fix a bug are now available.

The tcp_wrappers package provides small daemon programs which can monitor and filter incoming requests for systat, finger, FTP, telnet, rlogin, rsh, exec, tftp, talk and other network services. It also contains the libwrap library that adds the same filtering capabilities to programs linked against it, like sshd and more.

These updated tcp_wrappers packages fix the following bug:

- when tcp_wrappers performed an ident query which failed, applications which used tcp_wrappers were then unable to receive SIGALRM (alarm) signals. This has been fixed by correctly restoring signal masks in this update, so that applications using tcp_wrappers are now able to receive and handle SIGALRM signals following a failed ident query.

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

1.222. tetex

1.222.1. RHBA-2009:1118: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1118

Updated teTeX packages that fix various bugs are now available.

TeTeX is an implementation of TeX. TeX takes a text file and a set of formatting commands as input, and creates a typesetter-independent DeVice Independent (dvi) file as output.

These updated packages fix the following bugs:

- TeTeX provides the lineno package, which could cause conflicts with tetex-lineno package that is packaged separately. This update fixes the package conflict.
- Universal symbols are now provided that allow users to install a particular TeX component regardless of the current TeX distribution.
- These updated teTeX packages no longer display warnings on verification.
- lamstex fonts are now included, which are needed for proper functionality of other TeX components.

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

1.223. tftp

1.223.1. RHEA-2009:1274: enhancement update

Updated tftp packages that add support for IPv6 and correct errors in documentation are now available.

The Trivial File Transfer Protocol (TFTP) is normally used only for booting diskless workstations. The tftp package provides the user interface for TFTP, which allows users to transfer files to and from a remote machine. The tftp-server package provides the server for TFTP which allows users to transfer files to and from a remote machine.

These updated packages make the following changes.

- tftp has been re-based to version 0.49. This applies several upstream feature updates and bug fixes, including, most importantly, support IPv6. (BZ#464096)
- two spelling corrections were made to the tftp server man page (in.tftpd.8) and the NAME section of both the client (tftp.1) and server man pages was edited. (BZ#501482)

All users of tftp-server should upgrade to these updated packages, which resolve these issues.

1.224. thunderbird

1.224.1. RHSA-2009:1126: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1126

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Several flaws were found in the processing of malformed HTML mail content. An HTML mail message containing malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code as the user running Thunderbird. (CVE-2009-1392, CVE-2009-1303, CVE-2009-1305, CVE-2009-1833, CVE-2009-1838)

Several flaws were found in the way malformed HTML mail content was processed. An HTML mail message containing malicious content could execute arbitrary JavaScript in the context of the mail message, possibly presenting misleading data to the user, or stealing sensitive information such as login credentials. (CVE-2009-1306, CVE-2009-1307, CVE-2009-1308, CVE-2009-1309)

A flaw was found in the way Thunderbird handled error responses returned from proxy servers. If an attacker is able to conduct a man-in-the-middle attack against a Thunderbird instance that is using a proxy server, they may be able to steal sensitive information from the site Thunderbird is displaying. (CVE-2009-1836)

Note: JavaScript support is disabled by default in Thunderbird. None of the above issues are exploitable unless JavaScript is enabled.

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.

1.224.2. RHSA-2009:0258: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0258

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Several flaws were found in the processing of malformed HTML mail content. An HTML mail message containing malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code as the user running Thunderbird. (CVE-2009-0352, CVE-2009-0353, CVE-2009-0772, CVE-2009-0774, CVE-2009-0775)

Several flaws were found in the way malformed content was processed. An HTML mail message containing specially-crafted content could potentially trick a Thunderbird user into surrendering sensitive information. (CVE-2009-0355, CVE-2009-0776)

Note: JavaScript support is disabled by default in Thunderbird. None of the above issues are exploitable unless JavaScript is enabled.

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.

1.225. tog-pegasus

1.225.1. RHBA-2009:1286: bug fix and enhancement update

Updated tog-pegasus packages that fix various bugs and add enhancements are now available.

OpenPegasus WBEM Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent DMTF standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.

These updated packages upgrade tog-pegasus to the more recent upstream version 2.7.2, which provides a number of bug fixes and enhancements over the previous packaged version. The OpenPegasus Feature Status page referenced below summarizes the changes in this version. (BZ#474458)

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

- the upstream documentation about using SSL with OpenPegasus shipped in the previous package was inaccurate and out-of-date. This updated package contains additional documentation in the file README.RedHat.SSL that describes how to configure and how to use SSL with OpenPegasus. (BZ#479038)
- when the out of process providers feature is enabled, OpenPegasus executes WBEM providers in a separate process from the WBEM server. This isolates the server from any problems in the providers. Previously, the tog-pegasus package installed OpenPegasus with this feature disabled. Now, OpenPegasus is installed with the out of process providers enabled by default, therefore making WBEM services more reliable. (BZ#455109)

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

1.226. tomcat

1.226.1. RHSA-2009:1164: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1164

Updated tomcat packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

It was discovered that the Red Hat Security Advisory RHSA-2007:0871 did not address all possible flaws in the way Tomcat handles certain characters and character sequences in cookie values. A remote attacker could use this flaw to obtain sensitive information, such as session IDs, and then use this information for

session hijacking attacks. (CVE-2007-5333)

Note: The fix for the CVE-2007-5333 flaw changes the default cookie processing behavior: with this update, version 0 cookies that contain values that must be quoted to be valid are automatically changed to version 1 cookies. To reactivate the previous, but insecure behavior, add the following entry to the "/etc/tomcat5/catalina.properties" file:

org.apache.tomcat.util.http.ServerCookie.VERSION_SWITCH=false

It was discovered that request dispatchers did not properly normalize user requests that have trailing query strings, allowing remote attackers to send specially-crafted requests that would cause an information leak. (CVE-2008-5515)

A flaw was found in the way the Tomcat AJP (Apache JServ Protocol) connector processes AJP connections. An attacker could use this flaw to send specially-crafted requests that would cause a temporary denial of service. (CVE-2009-0033)

It was discovered that the error checking methods of certain authentication classes did not have sufficient error checking, allowing remote attackers to enumerate (via brute force methods) usernames registered with applications running on Tomcat when FORM-based authentication was used. (CVE-2009-0580)

A cross-site scripting (XSS) flaw was found in the examples calendar application. With some web browsers, remote attackers could use this flaw to inject arbitrary web script or HTML via the "time" parameter. (CVE-2009-0781)

It was discovered that web applications containing their own XML parsers could replace the XML parser Tomcat uses to parse configuration files. A malicious web application running on a Tomcat instance could read or, potentially, modify the configuration and XML-based data of other web applications deployed on the same Tomcat instance. (CVE-2009-0783)

Users of Tomcat should upgrade to these updated packages, which contain backported patches to resolve these issues. Tomcat must be restarted for this update to take effect.

1.227. totem

1.227.1. RHBA-2009:1288: bug fix update

Updated totem packages that fix various bugs are now available.

The totem packages contain a movie player that uses GStreamer to play back films and music.

This updated package provides the following bug fixes and enhancements:

- the NarrowSpace browser plugin for Firefox advertized itself as QuickTime 7.0. Because the current version of QuickTime is 7.6, some websites require versions of QuickTime newer than 7.0. Previously, when visiting such a site, content would not be available to Firefox with the NarrowSpace plugin. NarrowSpace now advertizes itself as QuickTime 7.2, allowing Firefox to access content on a greater number of websites. (BZ#483122)
- the totem packages place files in the /usr/include/totem and /usr/include/totem/1 directories but previously, did not list those directories for creation. These directories would therefore be created during the installation process, but would remain unowned. The directories are now listed for creation and are therefore owned by the package. (BZ#481816)
- previously, the totem packages were only built against the latest gstreamer plugin base. The totem packages are now built against the latest gstreamer plugins from the "good" set as well, ensuring the widest multimedia support from high-quality, freely-licensed plugins. (BZ#450108)

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

1.228. tzdata

1.228.1. RHEA-2009:1214: enhancement update

Note

This update has already been released (prior to the GA of this release) as errata RHEA-2009:1214

A new tzdata package that updates Daylight Saving Time observations for Egypt is now available.

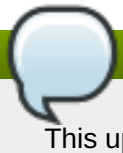
The tzdata package contains data files with rules for various time zones around the world.

This updated package addresses the following change to Daylight Saving Time (DST) observations:

- Egypt starts winter time on August 21. (BZ#517009 , BZ#517011 , BZ#517012)

All users, especially those in locales affected by these time changes and users interacting with people or systems in the affected locales, are advised to upgrade to this updated package, which adds these enhancements.

1.228.2. RHEA-2009:1105: enhancement update



Note

This update has already been released (prior to the GA of this release) as errata RHEA-2009:1105

A new tzdata package that updates Daylight Saving Time observations for Bangladesh is now available.

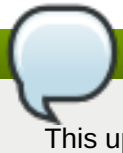
The tzdata package contains data files with rules for various time zones around the world.

This updated package addresses the following change to Daylight Saving Time (DST) observations:

- Bangladesh introduces DST on 20 June 2009. (BZ#503832 , BZ#503834 , BZ#503835)

All users, especially those in locales affected by these time changes and users interacting with people or systems in the affected locales, are advised to upgrade to this updated package, which adds these enhancements

1.228.3. RHEA-2009:0422: enhancement update



Note

This update has already been released (prior to the GA of this release) as errata RHEA-2009:0422

A new tzdata package that updates Daylight Saving Time observations in several locales is now available.

The tzdata package contains data files with rules for various time zones around the world.

This updated package addresses the following changes to Daylight Saving Time (DST) observations:

- Morocco will observe DST from 2009-06-01 00:00 to 2009-08-21 00:00.
- Tunisia will not observe DST this year.
- Syria started DST on 2009-03-27 00:00 this year.
- Cuba started DST at midnight between 2009-03-07 and 2009-03-08.
- the Province of San Luis, Argentina, went to UTC-04:00 on 2009-03-15.
- Palestine started DST on 2009-03-26 and end 2009-09-27.
- Pakistan will observe DST between 2009-04-15 and, probably, 2009-11-01.
- Egypt ends DST on 2009-09-24.

All users, especially those in locales affected by these time changes and users interacting with people or systems in the affected locales, are advised to upgrade to this updated package, which adds these enhancements.

1.229. udev

1.229.1. RHSA-2009:0427: Important security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0427

Updated udev packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

udev provides a user-space API and implements a dynamic device directory, providing only the devices present on the system. udev replaces devfs in order to provide greater hot plug functionality. Netlink is a datagram oriented service, used to transfer information between kernel modules and user-space processes.

It was discovered that udev did not properly check the origin of Netlink messages. A local attacker could use this flaw to gain root privileges via a crafted Netlink message sent to udev, causing it to create a world-writable block device file for an existing system block device (for example, the root file system). (CVE-2009-1185)

Red Hat would like to thank Sebastian Krahmer of the SUSE Security Team for responsibly reporting this flaw.

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

1.229.2. RHBA-2009:1346: bug fix and enhancement update

Updated udev packages that fix a bug and add an enhancement are now available.

The udev packages implement a dynamic device-directory, providing only the devices present on the system. This dynamic directory runs in user-space, dynamically creates and removes devices, provides consistent

naming, and a user-space API. udev replaces devfs, providing greater hot plug functionality.

These updated packages fix the following bug:

- leftover queue files from the udev instance of the initrd, caused a stall in the udev started from rc.sysinit. In this update the files are removed before starting the daemon in rc.sysinit. (BZ#487858)

These updated packages add the following enhancement:

- scsi_id was extended to query the ID of cciss devices, which do not provide information in the /sys filesystem. This enables the creation of persistent symbolic links in /dev/disk for cciss devices. (BZ#449057)

Users of udev are advised to upgrade to these updated packages, which resolve this issue and add this enhancement.

1.230. unix2dos

1.230.1. RHBA-2009:0294: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0294

Updated unix2dos2 packages that resolve a bug are now available.

The unix2dos utility converts UNIX text files to DOS or MAC format.

This updated package provides a fix for the following bug:

- when unix2dos created a new file as the output of its conversion (when run with the -n option), the new file would always have its permission mode set as 600, regardless of the permission mode of the original file. Unix2dos now sets the permission mode for the new file to be the same as the mode of the old file, filtered through the user's umask.

Users of unix2dos should upgrade to this updated package, which resolves this issue.

1.231. util-linux

1.231.1. RHBA-2009:1405: bug fix update

Updated util-linux packages that fix various bugs are now available.

The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, util-linux contains the fdisk configuration tool and the login program.

The updated packages include the following fixes:

- A previous version of the utility contained a scriptlet error in the post-install spec file.

The scriptlet error produced unnecessary error messages during the package installation process. With this update, the post-install spec file error messages are removed. (BZ#501870)

- The man page for raw(8) incorrectly stated that raw device support was deprecated. This update reinstates the raw device support information. (BZ#509334)

Users of util-linux should upgrade to these updated packages, which resolve these issues.

1.232. vim

1.232.1. RHBA-2009:1117: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1117

Updated vim packages that resolve several issues are now available.

VIM (VIsual editor iMproved) is an updated and improved version of the vi editor.

These updated vim packages provide fixes for the following bugs:

- autocommands are macro-like commands that the Vim editor runs when certain defined events occur, such reading or writing a certain file, leaving a buffer or window, or exiting Vim. Certain autocommands are provided with the vim package in Red Hat Enterprise Linux. However, if the user wanted to remove these autocommands, it was not easy to cleanly do so. With this update, the Red Hat-bundled autocommands are grouped into the "redhat" augroup, which allows the set of commands to be more easily manipulated or removed. (BZ#241308)

- on 32-bit architectures, Vim calculated the total amount of available memory incorrectly. This miscalculation resulted in Vim slowing down significantly when opening large files. With these updated packages, Vim now calculates the total amount of available RAM differently, which avoids the potential slowdown when opening and/or working with very large files. (BZ#429208)

- the package-provided vim.sh and vim.csh setup scripts in the /etc/profile.d directory, for the Bash and Tcsh shells respectively, employed incorrect shell scripting constructions that did not properly test certain conditions, such as whether strings returned by the "id" command could be empty. This update provides corrected setup scripts that fix these coding errors. (BZ#459823)

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

1.233. vino

1.233.1. RHEA-2009:1121: enhancement update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHEA-2009:1121

An enhanced vino package is now available.

Vino is a VNC server for GNOME. It allows remote users to connect to a running GNOME session using VNC.

This updated vino package adds the following enhancement:

- in the previous vino package, there were no visual indicators when someone was connected to your desktop. In this updated package, a status icon appears whenever someone is connected. (BZ#426256)

Users of vino are advised to upgrade to this updated package, which adds this enhancement.

1.234. virt-manager

1.234.1. RHBA-2009:1285: enhancement and bug fix update

An updated virt-manager package that fixes several bugs and adds enhancements is now available.

The Virtual Machine Manager (virt-manager) package provides a graphical tool for administering virtualized guests running on the Xen and KVM hypervisors. The virt-manager application uses the libvirt API to manage virtualized guests and hypervisors.

Bugs fixed in the updated virt-manager package include:

- Fully virtualized guests created with virt-manager are sometimes affected by a bug that prevents the mouse from moving freely throughout the screen. To work around this issue configure a USB tablet device for the guest with virt-manager. (BZ#223805)
- The virt-manager help documentation was out-of-date and broken. Presently, the documentation has been removed from the virt-manager to address the various issue and the 'help' buttons and menu items have been removed. Updated documentation is in development and may be available with future releases. (BZ#448716 , BZ#443628 , BZ#460713)
- Running virt-manager in unprivileged mode listed guests twice when connecting to remote hosts. If the remote host was disconnected and reconnected the list would double again. Every guest entry, including the duplicate entries could activate the guest. This issue is now resolved and only the available guests will be listed for a remote host. (BZ#448885)
- virt-manager would hang when attempting to connect to a Xen hypervisor with SSH. The updated virt-manager package has enhanced remote connection awareness and this issue no longer presents. (BZ#484063)
- Adding or removing a device during the guest installation procedure sometimes caused the guest to become unbootable. This behavior has been fixed in the updated package and devices can be added or removed during the installation. (BZ#472600)
- Changing memory allocation for running guests in virt-manager had no effect. This issue is resolved in the updated package and memory changes update correctly. (BZ#484314)
- Migrations with the virt-manager Migrate option failed due to incorrect parameters being sent to libvirt. The correct parameters are sent in the updated package. (BZ#509135)

This updated virt-manager package provides the following enhancements:

- virt-manager has been rebased to support the KVM hypervisor. (BZ#489374)
- Users can now add a sound for virtualized guests on the KVM hypervisor. Sound cards are optional for virtualized guests. The only available and default sound card device is an emulated AC97 device. (BZ#506035)

- the updated virt-manager package includes a storage management interface. Access the storage management interface by selecting the Edit->Host Details->Storage menu. The storage management interface manages local and networked storage devices.
- Graphical guest consoles support resizing and scaling.
- Users can view and remove virtualized sound, serial, parallel, and host devices from virtualized guests.
- Users can add sound cards and host devices to existing virtualized guests.
- The disk and network device model can be selected when adding new device to a virtualized guest.
- The default boot device for a virtualized guest can be selected in virt-manager. (BZ#484068)
- VTd and PCI passthrough are now supported. The VT-d feature provides hardware support for directly assigning physical PCI devices to a guest. The main benefit of the feature is to improve the performance of guest I/O to bare-metal levels for assigned PCI devices. Supported architectures for VTd include: 32 bit x86, 64-bit Intel EM64T and 64-bit Intel Itanium 2. (BZ#480521)

Users of virt-manager are advised to upgrade to this updated package, which provide these bug fixes and enhancements.

1.235. virt-viewer

1.235.1. RHBA-2009:1299: bug fix update

A updated virt-viewer package that fixes two issues with the "-w" option is now available for Red Hat Enterprise Linux 5.

Virtual Machine Viewer provides a graphical console client for connecting to virtual machines. It uses the GTK-VNC widget to provide the display, and libvirt for looking up VNC server details.

This update addresses the following two bugs:

- the "-w" or "--wait" options (for "wait for domain to start") returned an "invalid option" error rather than waiting for the nominated domain to start. (BZ#444024)
- when a guest was started up, running "virt-viewer --wait [guestname]" did not result in notification of the guest's changed status and did not result in virt-viewer connecting to the newly-started guest. (BZ#444028)

All Virtual Machine Viewer users should install this updated package which fixes these two problems.

1.236. vnc

1.236.1. RHSA-2009:0261: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0261

Updated vnc packages to correct a security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

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.

An insufficient input validation flaw was discovered in the VNC client application, vncviewer. If an attacker could convince a victim to connect to a malicious VNC server, or when an attacker was able to connect to vncviewer running in the "listen" mode, the attacker could cause the victim's vncviewer to crash or, possibly, execute arbitrary code. (CVE-2008-4770)

Users of vncviewer should upgrade to these updated packages, which contain a backported patch to resolve this issue. For the update to take effect, all running instances of vncviewer must be restarted after the update is installed.

1.237. vsftpd

1.237.1. RHBA-2009:1068: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1068

An updated vsftpd package that fixes a bug is now available.

The vsftpd package includes a Very Secure FTP (File Transfer Protocol) daemon.

This updated vsftpd package fixes the following bug:

- previously, the length of vsftpd usernames was limited to 32 characters in length. With this updated package, the maximum length of vsftpd usernames has been increased to 128 characters. (BZ#496846)

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

1.237.2. RHBA-2009:1282: bug fix update

A vsftpd update that increases the maximum username length and fixes several bugs is now available.

The vsftpd package deploys the Very Secure File Transfer Protocol daemon. This daemon enables secure and fast FTP service on Unix-like systems, providing SSL encryption, IPv6, bandwidth throttling, PAM integration, virtual users, virtual IPs and per-user/per-IP configuration.

This update applies the following bug fixes:

- in Red Hat Enterprise Linux 5, the default value for the 'background' option was changed to 'NO'. This revealed a race condition in the way vsftpd processed signals whenever child processes were forked. As a result of this race condition, attempts to run vsftpd could fail without returning an error code if another FTP service was also running. In this situation, a user would not be notified that vsftpd failed to run. This update implements extra routines for signal handling that fixes the race condition, ensuring that vsftpd returns a proper error code whenever it fails to start. (BZ#236707)

- the init script for this update is now POSIX-compliant. This corrects a bug that could cause vsftpd to incorrectly return a zero exit code when it failed to start. (BZ#431451)

- a bug in the dependencies between vsftpd parent and child processes allowed those child processes to

run even though their parent process was already terminated. As such, terminating the vsftpd service did not reliably stop all FTP connections initiated by vsftpd, which could pose a security risk. This update fixes the child-parent process dependency bug by adding several functions that terminate all vsftpd child processes whenever their parent process is stopped. (BZ#441485)

- a bug caused the vsftpd daemon to not properly shut down SSL (Secure Socket Layer) data connections, which led to interoperability problems between the vsftpd daemon and client programs such as FileZilla. This has been fixed in this update so that vsftpd no longer causes problems with client applications. (BZ#459607)
- in previous versions of vsftpd, /etc/vsftpd/vsftpd.conf specified /var/log/vsftpd.log as its default log file. However, this was different from the specified default log file (i.e. /var/log/xferlog) in /etc/logrotate.d/vsftpd.log. This prevented the logrotate script from finding -- and consequently, rotating -- the vsftpd log file, resulting in an unnecessarily large vsftpd log. This update corrects this issue by specifying /var/log/xferlog as its default log file in /etc/vsftpd/vsftpd.conf, which enables log rotation on vsftpd log files. (BZ#460067)
- this update also fixes several typographical errors in the documentation of some parameters in the vsftpd man page. (BZ#478526)
- vsftpd cannot locate usernames specified by the chown_username parameter if the username is trailed by whitespace. This update contains a workaround that trims trailing whitespaces from username values of chown_username. (BZ#486259)
- the maximum username length is now 128 characters. In previous versions, the maximum username was only 32 characters. (BZ#486524)
- the DNS reverse lookup feature was implemented without any way to disable it. This update contains the parameter 'reverse_lookup_enable', which allows users to enable or disable the DNS reverse lookup functionality. (BZ#498548)

Users of vsftpd are advised to upgrade to this update.

1.238. watchdog

1.238.1. RHEA-2009:1327: enhancement update

A watchdog update (re-based to upstream version 5.6) that applies several fixes and enhancements is now available.

The watchdog package provides a user-space application which can be configured to provide updates to a hardware or software watchdog timer via the Linux kernel's watchdog interface.

This version of the watchdog package is now re-based to upstream version 5.6. (BZ#446123)

This re-base several bug fixes and enhancements, including:

- The watchdog package was missing a required file, MNTTAB. This made it possible for watchdog to crash when the mnt_off() function initiated a shutdown. The missing MNTTAB file is now included with this version, thereby avoiding any possible crashes.
- /usr/share/doc/watchdog-5.6/examples/another-chance.sh script is now included. This script can be used as a repair binary, which can allow for several test failures before finally rebooting.
- Several bugs in the wd_keepalive program are now fixed. With this release, wd_keepalive now honors all command line options. In addition, wd_keepalive now requires a watchdog device to be configured properly.

Users of watchdog are advised to upgrade to this new version.

1.239. wdaemon

1.239.1. RHBA-2009:1111: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:1111

An updated wdaemon package that fixes a bug is now available.

wdaemon is a helper application which emulates persistent input devices for Wacom tablets so as to allow them to be plugged-in and unplugged while an X.org server is running.

This updated wdaemon package fixes the following bug:

- when starting the wdaemon service, the startup script printed an extraneous line giving the version of the program. This has been corrected in this updated package so that the wdaemon startup script is silent and thus conforms to the behavior of other daemon initialization scripts. (BZ#489050)

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

1.240. wget

1.240.1. RHBA-2009:1280: bug fix update

An updated wget package that fixes several bugs is now available.

GNU Wget is a file retrieval utility that can use either the HTTP or FTP protocols.

This package rebases Wget from version 1.10.2 to version 1.11.4 and fixes several bugs:

- the --recursive option would fail to retrieve any files; only a directory listing. (BZ#286161)
- Wget would ignore the --directory-prefix option (-P) if the server returned the header "Content-Disposition". Wget would then save the retrieved files in the current working directory, instead of the directory specified. (BZ#436822)
- the --mirror option would fail to retrieve files from FTP servers; only a directory listing (BZ#459679)
- the --no-content-disposition option would cause Wget to fail with the message "init.c:612: setval_internal: Assertion `0 <= comind && comind < (sizeof (commands) / sizeof ((commands)[0]))' failed." (BZ#492672)
- Wget would ignore the --no-clobber (-nc) argument and download files a second time. (BZ#475900)

All users of wget should upgrade to this updated package, which fixes these and other bugs, and adds numerous enhancements. For full details of bugs fixed in and features added to Wget between versions 1.10.2 and 1.11.4, refer to the upstream NEWS files available from the Wget website referenced below.

1.241. wireshark

1.241.1. RHSA-2009:1100: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:1100

Updated wireshark packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

A format string flaw was found in Wireshark. If Wireshark read a malformed packet off a network or opened a malicious dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2009-1210)

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malicious dump file. (CVE-2009-1268, CVE-2009-1269, CVE-2009-1829)

Users of wireshark should upgrade to these updated packages, which contain Wireshark version 1.0.8, and resolve these issues. All running instances of Wireshark must be restarted for the update to take effect.

1.241.2. RHSA-2009:0313: Moderate security update

Important

This update has already been released (prior to the GA of this release) as the security errata RHSA-2009:0313

Updated wireshark packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

Multiple buffer overflow flaws were found in Wireshark. If Wireshark read a malformed packet off a network or opened a malformed dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2008-4683, CVE-2009-0599)

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malformed dump file. (CVE-2008-4680, CVE-2008-4681, CVE-2008-4682, CVE-2008-4684, CVE-2008-4685, CVE-2008-5285, CVE-2009-0600)

Users of wireshark should upgrade to these updated packages, which contain Wireshark version 1.0.6, and resolve these issues. All running instances of Wireshark must be restarted for the update to take effect.

1.242. xen

1.242.1. RHBA-2009:1092: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1092

Updated xen packages that resolve an issue are now available.

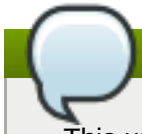
Xen is a high performance and secure open source virtualization framework. Virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

These updated xen packages fix the following bug:

- the Linux bonding driver aggregates multiple network interfaces into a single, local "bonded" interface. The 802.1Q specification (also known as VLAN tagging) allows multiple bridged networks to transparently share a single physical network link. When attempting to use a bonded interface and 802.1Q VLAN tagging together, the "network-bridge-bonding" networking script incorrectly called the ifdown command on interfaces other than "bond0", with the result that only the bond0 bridge became active (and not, for example, the "bond0.5" bridge). With these updated packages, using interface bonding together with 802.1Q VLAN tagging works as expected and all interfaces that are expected to become active do so, thus resolving the issue.

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

1.242.2. RHBA-2009:0401: bug fix update



Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:0401

Updated Xen packages that fix various bugs are now available.

Xen is a high performance and secure open source virtualization framework. Virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

Bugs fixed in these updated packages include:

- Data corruption occurred on guests with virtual SCSI disks larger than 1TB. This update adds support for virtual disks larger than 1TB.
- Various SCSI device data corruption issues occurred on fully virtualized guests with over 4GB of RAM. This update resolves the data corruption issues on fully virtualized guests with over 4GB of RAM.
- The Xen SCSI driver scsi_write_data() system call did not verify data if was written before returning. The SCSI driver now flushes the buffer before it returns which ensures data is written to the disk.

Users of Xen are advised to upgrade to these updated packages, which fix these bugs.

1.242.3. RHBA-2009:1328: bug fix and enhancement update

Updated xen packages that fix several bugs and add enhancements are now available.

The xen packages contain tools for managing the virtual machine monitor in Red Hat Enterprise Linux Virtualization.

These updated packages fix the following bugs:

- fix CPUs pinning in guest's configuration after save/restore sequence (BZ#228890)
- kernel command line could not be edited in IA64 PV guests during boot (BZ#249791)
- disallow migration for domains with attached PCI devices (BZ#334821)
- give memory back to dom0 if autoballooning failed (BZ#345271)
- credit scheduler parameters were not preserved during guest restart (BZ#345321)
- exclusively used devices could be attached to more than one guest at a time (BZ#345441)
- allow HVM guests creation under tight memory conditions (BZ#419771)
- migration of PV guests could hang on failure (BZ#428691)
- xend and xendomains init scripts returned wrong exit codes (BZ#430904)
- vfb and vkbd entries were not removed from xenstore after destroying a guest (BZ#439182)
- saving a guest reported success even if the operation failed (BZ#451675)
- the "xm console" documentation was updated to mention Ctrl-] sequence which escapes from xenconsole (BZ#454611)
- creating a guest could fail under heavy I/O in dom0 (BZ#456926)
- serialize iptables calls in hotplug scripts (BZ#460410)
- HVM guests suffered from missing clock interrupts (BZ#465116)
- P-V guests could not be rebooted after restarting xend (BZ#468971 , BZ#474579)
- Xen network-bridge script didn't work when source address was specified for default route (BZ#475249)
- passing out-of-range identification of an IDE disk caused a guest to misbehave or crash (BZ#475433)
- bogus MAC address was allowed to be specified for a virtual NIC (BZ#476611)
- data corruption occurred on guests with virtual SCSI disks larger than 1TB (BZ#479339)
- HVM guests suffered from time skews (BZ#480689)
- avoid SCSI device data corruptions on HVM guests with >4GB RAM (BZ#480843)
- flush Xen SCSI driver buffer to disk before returning from scsi_write_data() function (BZ#481782)
- correctly handle device detach attempts for devices mounted in guest (BZ#484110)
- "xm dump-core" didn't truncate existing files (BZ#484346)
- QCOW images were created with wrong byte order (BZ#485471)
- P-V guest didn't resume after failed save or migration (BZ#486157)
- xenconsole didn't work after failed save or migration (BZ#486291)
- QCOW images couldn't be used with PV guests or HVM guests with PV drivers (BZ#486353)

- xend didn't stop in runlevels 0, 1, and 6 (BZ#490053)
- libxenstore would leak memory on every @domainIntroduced event (BZ#490158)
- boot first entry in guest's grub.conf if default boot configuration is invalid (BZ#490754)
- pygrub would ignore "default" and "timeout" options in elilo.conf (BZ#491408)
- bridged network didn't work well when used together with bonding and 802.1q VLANs (BZ#492258)

These updated packages add the following enhancements:

- support for F11 and F12 keys in HVM BIOS (BZ#338321)
- support for Ctrk-Alt-Del in HVM BIOS (BZ#338331)
- support for global default keymap setting (BZ#345251)
- support for save, restore, migration and dump-core of 32b guests on a 64b host (BZ#425411 , BZ#480118)
- support for attaching PCI devices to HVM guests using VT-d (BZ#480520)
- support for virtual SCSI disks larger than 2TB (BZ#482780)
- support for local migrations (BZ#484967)
- support for 1GB host page tables (BZ#487342)
- support for relative mouse offset VNC extension (BZ#487559)
- support for INT13 LBA48 extensions in HVM BIOS (BZ#487907)
- fix PCIe NICs on Stoakley detach problem (BZ#507179)
- fix guest reboot with VT-d device assigned (BZ#507182)
- add BDFs duplicate check in HVM configure file (BZ#507195)
- fix MSI-X NIC hotplug removal (BZ#507198)
- fix `xm pci-list` BDF output on WeyBridge platform (BZ#507257)
- set cpu_weight default value back to 256 (BZ#508680)

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

1.243. xkeyboard-config

1.243.1. RHEA-2009:1369: bug fix and enhancement update

An xkeyboard-config package that fixes a bug and adds an enhancement is now available.

The xkeyboard-config packages provide the xkeyboard-config alternative xkb data files.

This update fixes the following bug:

- xkeyboard-config did not specifically recognize IBM Spacesaver keyboards that use a single key for both Num Lock and Scroll Lock. On these keyboards Shift-Scroll Lock is equivalent to the Num Lock keystroke.

Since the package did not recognize this equivalence it treated the Shift-Scroll Lock keystroke as other than Num Lock, making this keystroke unavailable. With this update, xkeyboard-config recognizes Spacesaver keyboards and properly handles their particular keyboard layout and keystroke idiosyncrasies. (BZ#442725)

As well, this updated package adds the following enhancement:

the pc105 keyboard model includes a number of multimedia key symbols. These keys are now supported by default. (BZ#432556)

- Users of xkeyboard-config are advised to upgrade to these updated packages, which address this bug and add this enhancement.

1.244. xorg-x11-drv-ati

1.244.1. RHBA-2009:1343: bug fix and enhancement update

An updated xorg-x11-drv-ati package that fixes bugs and adds enhancements is now available.

The xorg-x11-drv-ati package provides a driver for ATI cards for the X.Org implementation of the X Window System.e rhnsd init script returned incorrect error codes and sometimes prevented correct status command calls. The init script has been updated so that it returns appropriate error messages, and the status command call error no longer presents.

Bugs fixed in the updated package include:

- specifying NoDRI in the xorg.conf did not disable direct rendering on Red Hat Enterprise Linux 5.2 as expected. This has been corrected and specifying NoDRI in xorg.conf disables direct rendering on Red Hat Enterprise Linux 5.4. (BZ#465142)
- on Altix systems the FireMV card's second VGA output did not correctly detect a monitor plugged in. This has been corrected. (BZ#477679)
- graphical installation failed on ATI FireMV 2400 cards, although text-mode installations did work. With this update the r500 driver is now installed by default for FireMV 2400 cards and graphical installation now work as expected. (BZ#483165)
- on r600-based ATI cards (eg the Radeon 3100, the Radeon HD 3600 XT and Radeon Mobility HD 2600 Series cards) the mouse pointer could become corrupted. Note: this problem only appeared in Beta releases of Red Hat Enterprise Linux 5.4. It was not present in Red Hat Enterprise Linux 5.3 and was fixed for the public release of Red Hat Enterprise Linux 5.4 (BZ#514559)

The following enhancements are also included in the updated package:

- the r500 driver was updated to match the upstream X.org ATI 6.12.2 release. This added support for the latest ATI GPUs including the rs880. (BZ#495098) (BZ#477257)
- the r500 driver now supports the Xinerama extension, providing significantly improved support for multi-head setups, especially those involving displays with different aspect ratios. (BZ#481067)

All ATI graphics card users should upgrade to this updated package, which resolves these issues and adds these features.

1.245. xorg-x11-drv-i810

1.245.1. RHBA-2009:1391: bug fix and enhancement update

An updated xorg-x11-drv-i810 driver package that fixes various bugs and provides various enhancements is now available.

xorg-x11-drv-i810 is an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

Note that this package provides two drivers, 'i810' and 'intel'. The i810 driver is supported for i8xx series chips, up to and including i865. The intel driver is supported for all i915 and later chips.

This updated package provides the following bug fixes and enhancements:

- previously, support for switching between virtual terminals -- or between virtual terminals and the X Window System -- was not fully implemented for newer Intel graphics cards. Users experienced a wide range of problems when they switched, including: losing the display completely; having the display filled with random, pulsating colors; receiving "out of range" or "can't display this mode" errors; the system ceasing to respond; or the system restarting. Cards affected included those with the G4X, G965, GM45, Q43, and Q45 chipsets. The driver now includes full support for switching to, from, and between virtual terminals, meaning that users can switch safely without encountering the problems that they experienced previously. (BZ#244933 , BZ#470450 , BZ#487657)

- previously, no man page was provided to describe the "intel" driver included in this package, only the "i810" driver. A separate man page is now supplied for each driver. (BZ#467186)

- the graphics cards supported by the two drivers in this package overlap considerably. Previously, this created confusion for users as they selected the driver to use with a particular card. A preferred driver is now specified for each card, and if users select the non-preferred option, they receive a warning that the particular combination of card and driver is not a supported configuration. This clarifies the use of the drivers in this package. Existing configurations will continue to function, regardless of the combination of card and driver. (BZ#479067)

- Lenovo Thinkpad notebooks have a "Fn" key that can be combined with the numbered function keys to access a variety of features, typically including volume, screen brightness, sleep, and switching to an external monitor. Previously, these key combinations would not produce the desired outcomes on X61 Thinkpad notebooks. Although some of these functions were enabled by changes in other software components, no support existed within the graphics drivers for the key combinations that would brighten and dim the display. Support for these features is now present in the driver. X61 users can now use the hotkeys to control screen brightness on their notebooks. (BZ#468448)

- previously, although the code to support HDMI output was included in the driver, this was not initialized while the system detected displays. Therefore, the system was unable to detect monitors connected by DVI. HDMI detection is now enabled so that when the system initializes displays, the system can detect monitors on DVI connections and output to them correctly. (BZ#476831)

- previously, Xinerama mode was not enabled for the "intel" driver. Therefore, when users set Xinerama mode for a graphics card that uses the "intel" driver, the driver would crash. The "intel" driver now includes support for Xinerama, making this mode available to users. Note that a scrolling problem that users also experienced when using the "intel" driver for dual-head configurations was not related to this driver, and is resolved in a separate update for the X server. (BZ#477177)

All users of the xorg-x11-drv-i810 driver should upgrade to this updated package, which resolves these issues and adds these enhancements.

1.246. xorg-x11-drv-mga

1.246.1. RHBA-2009:1390: bug fix update

An updated xorg-x11-drv-mga driver which fixes several bugs is now available.

xorg-x11-drv-mga is a video driver for the X.Org implementation of the X Window System, for Matrox G-series chips.

This updated package provide the following bug fixes:

- the driver version written to the Xorg log file in /var/log/ did not reliably match the driver version in use. (The Xorg log file reported version 1.4.1 when the version in use was 1.4.2.) With this update, this error has been corrected and the Xorg log file reports the driver version accurately. (BZ#474209)
- some video cards based on the Matrox G200SE chip-set do not have enough installed RAM to support 24-bits per pixel (bpp) at 1024 x 768 pixels resolution. Previously, the xorg-x11-drv-mga driver automatically switched output to 16-bpp when a display being driven by such a card was running at 1024 x 768 (XGA) pixels resolution regardless of the amount of installed RAM. With this update, only cards with 2 MB of RAM or less are automatically switched to 16-bpp. Matrox G200SE-based video cards with more installed RAM can now display 24-bpp at 1024 x 768. (BZ#479919)
- the limited bandwidth of the G200SE chip-set caused some 24-bit color modes to be rejected when using the default 32-bpp framebuffer. With this update, a 24-bpp packed framebuffer is now the default for G200SE-based cards. This reduces the bandwidth required and allows otherwise rejected modes to work. Note: the 32-bpp framebuffer is still the default for other chip-sets. (BZ#508039)

All xorg-x11-drv-mga users should upgrade to this updated package which addresses these issues.

1.247. xorg-x11-drv-nv

1.247.1. RHEA-2009:1342: enhancement update

An enhanced xorg-x11-drv-nv package is now available.

xorg-x11-drv-nv provides a driver for NVIDIA cards for the X.org implementation of the X Window System.

This update resolves the following bug:

- NVIDIA Quadro FX 570 and Quadro FX 1700 graphics cards obtain modetimings from the X server for mode validation ("native modesetting"). Previously, xorg-x11-drv-nv did not support native modesetting, and therefore would not work with these cards. With native modesetting supported in xorg-x11-drv-nv, this driver now works with Quadro FX 570 and Quadro FX 1700 graphics cards. (BZ#480025)

This update also adds support for:

- switching between internal and external displays with the Fn+F7 key combination on Lenovo T61p notebooks. (BZ#435285)
- NVIDIA GeForce 9800GTX graphics cards. (BZ#452996)

All users of NVIDIA graphics cards should install this package, which resolves this issue and adds these enhancements.

1.248. xorg-x11-proto-devel

1.248.1. RHEA-2009:1411: enhancement update

An updated xorg-x11-proto-devel package is now available.

The xorg-x11-proto-devel package provides X.Org X11 Protocol header files that are used when building X servers or X client libraries.

Previously, the XFD_SETSIZE value in the Xpoll.h header file was set to allow only 256 X client connections for a single X server. Consequently, if this limit was reached, the X Server would silently deny new connections. With this update, the XFD_SETSIZE has been modified to support a maximum of 512 X client connections. The X server supplied in Red Hat Enterprise Linux 5.4 has been built with this limit increase included. (BZ#511913)

All users of xorg-x11-proto-devel are advised to install this updated package, which provides this enhancement.

1.249. xorg-x11-server

1.249.1. RHBA-2009:1373: bug fix and enhancement update

Updated xorg-x11-server packages that fix bugs and add enhancements are now available.

X.org X11 is an open source implementation of the X Window System. It provides the basic low level functionality upon which full fledged graphical user interfaces such as GNOME and KDE are designed.

These updated packages address the following bugs:

- an error in trapezoid rasterisation that caused X to crash and which could be triggered on large web pages has been fixed. (BZ#448586)
- a crash in software image transfers on 64-bit systems that caused Xvfb (the X virtual framebuffer) to segfault has been fixed. (BZ#467370)
- a 64-bit bug in the x86 emulator that prevented X from starting on AMD64 and Intel 64 clients was corrected. (BZ#503072)
- the xorg-x11-server-randr-source package is obsolete but no other packages "obsolete" it. With this update xorg-x11-server obsoletes the randr-source package and, if the old package is present, installing this update will remove it automatically. (BZ#503072)

This update also includes the following enhancements:

- the -maxclients command line option was added to the X server. This option allows for configurations with either more clients or more resources per client. (BZ#439797)
- two new opcodes to support newer video BIOSes were added. Note: Intel Mobile Express Series 5 chipsets (also known as "Ironlake graphics" for the CPU used with the chipsets) are only supported in VESA mode in Red Hat Enterprise Linux 5. (BZ#503182)

All xorg-x11-server users should upgrade to these updated packages, which resolve these issues and add these features.

1.250. yaboot

1.250.1. RHBA-2009:1386: bug fix and enhancement update

An updated yaboot package that fixes a bug and adds an enhancement is now available.

The yaboot package is a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

This updated package fixes the following bug:

- previously the debuginfo rpm of yaboot was built but the built package was empty. yaboot contains ELF

objects but is neither a Linux nor a Mac OS X executable file: it is meant to be executed by OpenFirmware only. With this update the debuginfo rpm is, correctly, not built at all. (BZ#500639)

This update also adds the following enhancement.

- support for handling IPv6 boot parameters has been added to yaboot, which now supports booting and operating system installation over IPv6. (BZ#475807)

All PowerPC yaboot users are advised to upgrade to this updated package, which resolves these issues.

1.251. ypbind

1.251.1. RHBA-2009:0462: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0462

An updated ypbind package that fixes a bug is now available.

This package provides the ypbind daemon. The ypbind daemon binds NIS clients to a NIS domain. Systems running NIS client programs must have ypbind running.

This updated ypbind package fixes the following bug:

- the ypbind(8) manual page did not contain a description of the '-p [port]' option, which is used to specify the port to which ypbind binds. (BZ#474184)

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

1.252. yum

1.252.1. RHBA-2009:1142: bug fix update

Note

This update has already been released (prior to the GA of this release) as errata RHBA-2009:1142

An updated yum package that resolves an issue with RHN Snapshot Rollback is now available.

Yum is a utility that can check for or automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as necessary.

This updated yum package fixes the following bug:

- attempting to roll back a system to a previous configuration by selecting the "Rollback to Snapshot" function on the RHN System Details page could cause the removal of packages which should have been downgraded instead. With this updated package, this situation is now handled gracefully, and packages are correctly downgraded in accordance with the rollback package manifest. (BZ#503944)

All users of yum and Red Hat Network are advised to upgrade to this updated package, which resolves this

issue.

1.252.2. RHBA-2009:1419: bug fix update

An updated yum package that fixes various bugs, adds a number of features and contains optimizations is now available.

Yum is a utility that can check for or automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as necessary.

- Several typos in **yum** manual pages have been corrected. (BZ#447588, BZ#510012)
- **Yum** now includes support for X.509 authentication at both the server and client end. This allows users of **yum** with custom respositories to implement this increased layer of security. (BZ#462915)
- The rebased code in this version of **yum** handles the removal of **`.sqlite`** files differently from older versions. Previously, **yum** could crash while completing a transaction if it were still cleaning up the **`.sqlite`** file from a previous transaction. This crash cannot happen in the current version of **yum**. (BZ#470274)
- Previously, **yum** did not create a **`pkgSack`** object for a transaction if the transaction included both a removal and an installation of the same package. As a result, the transaction would fail with the message **`Error: Transaction Check Error: package package_name is already installed`**. Now, **yum** creates a **`pkgSack`** object for the transaction, removes the package, and reinstalls it. (BZ#471207)
- Previously, due to the constraints of a default terminal screen with a width of 80 characters, the **`yum repolist command`** would truncate the results of both the **`repo id`** and **`repo name`** columns. Because the beginnings of many channel ids and and names are identical, the truncation could make it impossible to identify specific channels. **Yum** now displays the **`repo id`** column in its entirety, although the **`repo name`** column is even further truncated. However, with at least one of these columns displayed in full, it is now possible to positively identify specific channels. (BZ#471598)
- Previously, **yum** assumed that any terminal was 80 characters in width. Therefore, when it drew a progress bar on the screen, each additional # printed would force a new line on terminals narrower than 80 characters. **Yum** now determines the actual width of the terminal rather than assuming the width, and draws its progress bars accordingly. (BZ#474822)
- Previously, when in quiet mode, **yum** would not print details of the transaction, only the prompt **`Is this ok [y/N]`** . Under certain circumstances, messages from plugins (such as the RHN plugin) might appear directly above the prompt in quiet mode and make it appear as if the prompt were related to the message from the plugin rather than to the transaction. **Yum** now now always prints details of the transaction -- even in quiet mode -- so that it is always obvious to what the prompt is referring. (BZ#474826)
- Because **yum** does not lock **`rpmdb`**, other applications can make changes to the package database at the same time that **yum** does. Previously, changes made to **`rpmdb`** by another application could cause **yum** to crash; for example, if an application removed data about a package and **yum** then attempted to retrieve this data. Now, if **yum** discovers data that is needs to complete a transaction is missing from the **`rpmdb`**, **yum** will exit safely and avoid crashing. (BZ#476195)
- Previously, if a plugin modified a **yum** transaction with a postresolve hook, **yum** would ignore problems created by the original transaction. If the original transaction included conflicting packages, **yum** would be unable to resolve the conflict and the transaction would fail. Now **yum** does not ignore problems created by the original transaction in situations where the transaction is modified by a plugin and is able to resolve conflicts as it normally would. (BZ#481164)
- Previously, when used with the **`--disablerepo='*'`** option, or when available repos had no packages in them, the **`yum install '*'`** command produced a long warning that listed every package already on

the system as being installed and not available. This warning was nonsensical and misleading because it implied that every package already on the system was available in a repository that yum could access. The code that produced this warning has been removed from **yum**. Now when yum install '*' is used under circumstances where no packages are available in any repository, **yum** does not produce this warning, but simply reports **`Nothing to do`**. (BZ#482812)

- Previously, one of the tests that **yum** performed during a transaction produced erroneous results when rolling back a package on a managed system to an earlier version. The result of this test was that **yum** would remove the package altogether rather than roll it back. Since the test was redundant, it has been removed from **yum**, with the result that **yum** now rolls back packages on managed systems correctly. (BZ#489256)

- Current versions of yum include code for old **yum** utilities. The continued availability of the old utilities allows developers to ensure backward compatibility of **yum** features with the versions of **yum** shipped with earlier versions of Red Hat Enterprise Linux. A number of errors in this code have been corrected, ensuring that tests against these old utilities remain valid. (BZ#491077)

- Because every rpm package should have a **`%description`** field, **`yum info`** did not allow for packages where this field might be empty. When **`yum info`** encountered such a package, it would crash. **`Yum info`** now allows for empty **`%description`** fields in packages and will not crash when it encounters an empty field. (BZ#491406)

- Previously, when an old version of a package accidentally provided a capability, **yum** might still have picked newer versions of that package to provide that capability, even if the newer vesions did not provide the capability. As a result, **yum** could assume that a dependency was met, even when it was not. **Yum** now tests dependencies more carefully, preventing this situation from occurring and ensuring that dependencies are properly met. (BZ#498635)

- When **yum** installed local packages, it defaulted to expecting SHA-256 checksums. Because packages for Red Hat Enterprise Linux 5 use MD5 checksums, the installation would fail with a **`bad checksum type`** error. Now, when **yum** encounters a bad SHA-256 checksum, it attempts to verify the package with a SHA-1 checksum instead, which will sucessfully verify the MD5 checksums used for Red Hat Enterprise Linux 5 packages. (BZ#500697)

- Previously, when a user attempted a **`yum update`** for a package that was not installed, **yum** would exit with the message **`No Packages marked for Update`**, whether the package were available or not. Although true, this message did not alert the user that such a package was available for installation. Now, if the package is available but not installed, **yum** notifies the user of this fact. (BZ#507326)

- The Linux environment variable **`LC_CTYPE`** specifies a character set and the variable **`LC_MESSAGES`** specifies a language for messages. Previously, yum selected a language for messages based on **`LC_CTYPE`** instead of **`LC_MESSAGES`**. Although on many configurations, **`LC_CTYPE`** and **`LC_MESSAGES`** will be set to the same language and character encoding, this is not necessarily the case, and by using the wrong environment variable, yum would not provide the expected output under configurations where **`LC_CTYPE`** and **`LC_MESSAGES`** were set differently. Yum now uses **`LC_MESSAGES`** to determine the language to provide messages in, resulting in consistent and expected behavior. (BZ#507357)

- Due to a logic error in the code, **yum** ignored the **`--color=never`** option on the command line and **`color=never option`** in **`yum.conf`**. **Yum** output was therefore always in color, regardless of user preferences. With the error corrected, users can now use **yum** in monochrome. (BZ#507883)

- Under certain, unusual circumstances, **yum** could encounter an infinite recursion while executing the **`package-cleanup --dupes`** command. Yum would crash and the recursion would eventually terminate with the error **`maximum recursion depth exceeded while calling a Python object`**. The code that populates the package sacks is now modified so that this recursion cannot take place, therefore avoiding the crash. (BZ#507885)

- The method that **yum** uses to import the names of modules previously omitted the **`to_str`** parameter. Therefore, when loading the **yum-filter-data** plugin, **yum** crashed. With **`to_str`** now specified in the code, **yum** can import the module name and does not crash when it loads the plugin. (BZ#508051)
- Previously, the code used by **yum** to allow users to set repo directory attributes contained several flaws. As a result, attempts to set the download directory with the **`--downloaddir`** option resulted in a crash. The code used to set directory attributes is now substantially rewritten and now allows the **`--downloaddir`** option to work correctly. (BZ#508055)
- While populating the package sack, **yum** did not account for the possibility repos had been added where none existed before. Therefore, if the repos were not specified in the original configuration, and repos were subsequently added, **yum** would not add to the package sack the first time that it tried to use the new repos. This situation could lead to problems during installation or the creation of live CDs. **Yum** now re-initializes the package sack when a repo is added if no repo was previously specified. (BZ#508659)
- A recent version of **yum** was substantially slower than previous versions when calculating cost excludes. The slowdown was caused by variable that expanded to unicode encoding rather than str. The calculation no longer uses unicode, which returns **yum** to its previous higher speed. (BZ#500000)
- Some recent combinations of versions of **yum** and **rpm** produced conditions under which it was possible that **yum** would fail to recognize when **rpm** failed to install a package. Despite the failure, **yum** would report that the package had been updated. The rebase of **yum** to version 3.2.22 allows **yum** to detect **rpm** failures more reliably. (BZ#282951)

1.253. yum-metadata-parser

1.253.1. RHBA-2009:0440: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0440

An updated yum-metadata-parser package that fixes a bug is now available.

yum-metadata-parser is a fast metadata parser for yum implemented in C.

This updated yum-metadata-parser package fixes the following bug:

- in certain circumstances, yum-metadata-parser corrupted yum's sqlite database, which could have led to problems such as dependency resolution failures when attempting to upgrade packages. With this update, yum regenerates the sqlite database file following each repository metadata download, which solves possible database corruption issues.

All users should upgrade to this updated package, which resolves these issues by always generating the .sqlite files from scratch.

1.254. yum-rhn-plugin

1.254.1. RHBA-2009:1355: bug fix and enhancement update

An updated yum-rhn-plugin package that fixes several bugs is now available.

yum-rhn-plugin allows yum to access a Red Hat Network server for software updates.

This update fixes several bugs:

- the software updater (pup) did not parse OpenSSL error messages correctly. Therefore, when it encountered an invalid or missing SSL certificate, the updater would crash. The parsing code is now corrected, so invalid or missing SSL certificate will not result in a crash. (BZ#441738 , BZ#481042)
- /etc/sysconfig/rhn/systemid stores the identity of a system registered with the Red Hat Network. Previously, yum-rhn-plugin did not allow for situations where this file was missing, so would cause yum to crash when it could not find the file. If the systemid file is missing, the plugin now warns the user that the SystemID could not be acquired and that the system might not be registered on the Red Hat Network. (BZ#444581)
- previously, if yum itself was updated during an update transaction, the version of yum running in memory might attempt to read a yum.conf file that was updated for the new version of yum. If the new yum.conf file were incompatible with the old version of yum, yum would crash and the transaction would fail. Now, before running the transaction, yum creates a YumBase object to hold the actions and associated parameters that it will need during the transaction. By referring to this object, yum does not need to obtain configuration information during the transaction, and therefore avoids any incompatibility introduced by a change in the yum.conf file. (BZ#448245)
- yum-rhn-plugin creates creates a file at /var/spool/up2date/loginAuth.pkl that caches login information. If the contents of this file were to become corrupt, attempts to log in would result in a 404 error. Now, yum-rhn-plugin deletes this file at the end of each transaction and creates a new copy the next time that yum is run. Renewing this file ensures that cached login information is current and uncorrupted. (BZ#465340 , BZ#489396)
- previously, yum-rhn-plugin did not allow for situations where the update agent sent a request to a Red Hat Network server, but received no response within its timeout interval. This would generate an unhandled exception that would crash the update agent. Now, if the update agent does not receive a timely response from an RHN server, it will present the user with an error message that says: "Server Unavailable. Please try later". (BZ#467866)
- previously, while processing package removals, yum-rhn-plugin would not take architecture information into account. Therefore, on a system where a package was installed for more than one architecture, removing the package for one architecture would remove the package for all architectures. Yum-rhn-plugin now pays attention to the architecture of the package that is to be removed, and removes the package for only that architecture. (BZ#476899)
- yum-rhn-plugin did not account for missing dependencies while processing scheduled package actions from RHN hosted or satellite servers. If a dependency was missing in the channel, yum-rhn-plugin would report that the package was installed successfully, even though it failed. Now, yum-rhn-plugin notes missing dependencies, and correctly reports that installation of a package failed due to dependency problems. (BZ#491127)

All users of yum-rhn-plugin are advised to upgrade to this updated package, which resolves these issues.

1.255. zsh

1.255.1. RHBA-2009:0463: bug fix update

Note

This update has already been released (prior to the GA of this release) as FASTRACK errata RHBA-2009:0463

Updated zsh packages that fix various bugs are now available.

The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.

These updated zsh packages provide fixes for the following bugs:

- when running a large number of processes, it was possible for duplicate PID numbers to enter the job table. Under certain conditions, zsh would wait forever for a process with the same PID as another, finished process, to itself finish. With these updated packages, zsh is now able to determine when jobs with the same PID numbers are both finished, or not, or one is and not the other. (BZ#465455)

- zsh code blocks which started with the "$(" sequence and ended correctly with a closing parenthesis ")", but which contained comments, were parsed incorrectly. This has been fixed so that "$(..)" blocks which contain comments are still parsed correctly, thus resolving possible syntax errors in zsh commands and scripts. (BZ#484348)

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

Chapter 2. New Packages

2.1. RHEA-2009:1284: blktrace

A new package is now available for Red Hat Enterprise Linux 5.

blktrace is a block layer IO tracing mechanism which provides detailed information about request queue operations to user space.

This new package includes both **blktrace**, a utility which gathers event traces from the kernel; and **blkparse**, a utility which formats trace data collected by **blktrace**.

2.2. RHEA-2009:1325: celt051

A new **celt051** package providing low-latency audio encoding and decoding capabilities is now available.

Constrained Energy Lapped Transform (CELT) is an ultra-low delay audio codec designed for real-time transmission of high quality speech and audio.

The new **celt051** package provides the 0.5.1 protocol version of the CELT codec for applications that need low-latency audio streaming (e.g. the Spice hypervisor client protocol).

Users of Spice and those requiring application support of the CELT codec are advised to install this package.

2.3. RHEA-2009:1383: ctdb

A new **ctdb** package is now available.

CTDB is a clustered database based on Samba's Trivial Database (TDB). The ctdb package is a cluster implementation used to store temporary data. If an application is already using TBD for temporary data storage, it can be very easily converted to be cluster-aware and use CTDB. (BZ#499241)

Note

CTDB is included as a Technology Preview. Technology Preview features are included in Red Hat Enterprise Linux to provide the features with wide exposure, with the goal of supporting these features in a future release of Red Hat Enterprise Linux. Technology Preview features are not supported under Red Hat Enterprise Linux 5.4 subscription services, and may not be functionally complete. Red Hat welcomes customer feedback and suggestions for Technology Previews. Advisories will be provided for high-severity security issues in Technology Preview features.

All users requiring CTDB should install these newly released packages, which add this enhancement.

2.4. RHEA-2009:1276: etherboot

Etherboot, a new package that enables PXE-booting, is now available.

Etherboot provides the capability to boot guest virtual machines using the Preboot eXecution Environment (PXE). This process occurs before the operating system is loaded; in most cases, the operating system has no knowledge that it was booted through PXE. Many network adapters contain a socket where a ROM chip can be installed; this ROM chip is used to store PXE-boot code provided by **Etherboot**. At present,

Etherboot is only supported for use in KVM. (BZ#488612)

This version of Etherboot was compiled with the **POWERSAVE**, **PXE_DHCP_STRICT**, and **ASK_BOOT=-1** options. **PXE_DHCP_STRICT** is required by some network drivers to support PXE-booting, while the **ASK_BOOT=-1** option prevents a guest from consuming too much CPU time during boot-up. The **POWERSAVE** option reduces CPU consumption on a host whenever a guest performs a PXE-boot. (BZ#481914 and (BZ#500894)

2.5. RHEA-2009:1318: fcoe-utils

A new **fcoe-utils** package is now available for Red Hat Enterprise Linux 5.

The **fcoe-utils** package contains the **fcoeadm** command line utility, which is the Fibre Channel-over-Ethernet (FCoE) management tool for Linux systems. The fcoeadm utility can create, destroy and reset an FCoE instance on a given network interface, as well as retrieve and display information about FCoE instances.

This **fcoe-utils** package is new to Red Hat Enterprise Linux 5. (BZ#494555)

All Fibre Channel-over-Ethernet users requiring an administrative FCoE interface should install this newly-released package, which adds this enhancement.

2.6. RHEA-2009:1320: fuse

fuse, a new package that enables users to mount FUSE file systems, is now available.

FUSE (Filesystem in Userspace) is an interface for userspace programs to export a virtual file system to the Linux kernel. FUSE also aims to provide a secure method for non-privileged users to create and mount their own file system implementations.

FUSE, which can implement a fully functional file system in a userspace program, consists of three main parts: a kernel filesystem module; a userspace library; and a mount utility. This package contains the mount utility, fusermount; the FUSE userspace tool to mount FUSE file systems. BZ#252372)

Note

FUSE has no relationship with the ZX Spectrum emulator also known as Fuse.

Anyone looking to mount FUSE file systems or otherwise use FUSE should install this new package.

2.7. RHEA-2009:1297: gnupg2

A new package, **gnupg2**, which provides the GnuPG 2.0 cryptographic software suite, is now available for Red Hat Enterprise Linux 5.

GnuPG is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures. It includes an advanced key management facility and is compliant with the proposed OpenPGP Internet standard as described in RFC2440 and the S/MIME standard as described by several RFCs.

GnuPG 2.0 is a newer version of GnuPG with additional support for S/MIME. It has a different design philosophy that splits functionality up into several modules. (BZ#445420)

Users wishing to use this later version of GnuPG for secure communications should install this new package. Note: both version 1.x and version 2.0 may be installed simultaneously. In GnuPG 2.0, **gpg** is called **gpg2** and does not conflict with an installed 1.x OpenPGP-only version.

2.8. RHEA-2009:1281: hmaccalc

hmaccalc, a new package that processes HMAC values for authentication purposes, is now available.

The **hmaccalc** package provides tools that compute and verify hash-based message authentication code (HMAC) values for the contents of files. These tools process HMAC values using the SHA family of digest algorithms along with a user-specified key. (BZ#467500 and (BZ#491724)

2.9. RHEA-2009:1275: iasl

iasl, a new package that compiles ASL into AML, is now available. This package is a build requirement for KVM.

iasl compiles ACPI Source Language (ASL) into ACPI Machine Language (AML); it can also be used to de-compile AML for debugging purposes. AML is suitable for inclusion as Differentiated System Description Tables (DSDT) in system firmware. In addition, **iasl** is also used to build the BIOS images inside the KVM userspace source. As such, **iasl** is included in this release as a build requirement of the **kvm** package. (BZ#488614)

2.10. RHEA-2009:1272: kvm

A new **KVM** pacakge is available that adds a new hypvervisor for full virtualization is now available.

KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware.

KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems. KVM is a hypervisor which uses the **libvirt** virtualization tools (**virt-manager** and **virsh**).

The KVM hypervisor cannot run at the same time as the Xen hypervisor. Both hypervisors, Xen and KVM, can be installed on the same system, however, only one hypervisor can be used at a time.

KVM is only available for the Intel 64 and AMD64 architectures.

For more information on changing hypervisor or using KVM refer to the Red Hat Enterprise Linux Virtualization Guide.

All users requiring KVM should install this newly released package.

2.11. RHEA-2009:1296: libassuan

A new package, **libassuan**, is now available for Red Hat Enterprise Linux 5.

libassuan is a small library that implements the Assuan protocol. The protocol, which provides a server and client interface, is used for Inter-process Communication (IPC) between newer GNU Privacy Guard (**gnupg2**) components.

This new package is required by the new **gnupg2** utility. GnuPG 2.0 is a newer version of GnuPG, a tool for secure communication and data storage. GnuPG 2.0 derives from a different design philosophy and includes additional support for S/MIME. (BZ#484192)

The package also addresses the following pre-release bug:

- * a multilib conflict in the **`libassuan-1.0.4-4.el5`** package is now resolved. (BZ#502677)

Users of **gnupg2** are advised to upgrade to these updated **libassuan** packages, which resolve these issues.

2.12. RHEA-2009:1314: libhbaapi

A new **libhbaapi** package is now available for Red Hat Enterprise Linux 5.

The **libhbaapi** library is the Host Bus Adapter (HBA) API library for Fibre Channel and Storage Area Network (SAN) resources. It contains a unified API that programmers can use to access, query, observe and modify SAN and Fibre Channel services.

This **libhbaapi** package is new to Red Hat Enterprise Linux 5. (BZ#494548)

All users who require a unified programming interface to Fibre Channel HBA information should install this newly-released package, which adds this enhancement.

2.13. RHEA-2009:1316: libhbalinux

A new **libhbalinux** package is now available for Red Hat Enterprise Linux 5.

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**.

This **libhbalinux** package is new to Red Hat Enterprise Linux 5. (BZ#494550)

All users requiring **libhbalinux** should install this newly-released package, which adds this enhancement.

2.14. RHEA-2009:1295: libksba

A new package, **libksba**, is now available for Red Hat Enterprise Linux 5.

KSBA is a library designed to build software based on the X.509 and CMS protocols. It provides developers with a single API that handles the underlying details of the X.509 protocol and presents data consistently.

This new package is required by the new **gnupg2** utility. GnuPG 2.0 is a newer version of GnuPG, a tool for secure communication and data storage. GnuPG 2.0 derives from a different design philosophy and includes additional support for S/MIME. (BZ#484191)

Anyone wishing to use GnuPG 2 is advised to also install this new package.

2.15. RHEA-2009:1315: libpciaccess

A new **libpciaccess** package is now available for Red Hat Enterprise Linux 5.

The **libpciaccess** library provides simple access to information about PCI devices and their configuration. This library works across multiple operating systems and is utilized by the **libhbalinux** library. On Linux, **libpciaccess** uses either the sysfs virtual file system or the **`/dev/mem device`** to communicate with PCI devices.

This **libpciaccess** package is new to Red Hat Enterprise Linux 5. (BZ#496211)

All users requiring **libpciaccess** should install this newly-released package, which adds this enhancement.

2.16. RHEA-2009:1326: log4cpp

A new **log4cpp** package is now available.

log4cpp is a library of C++ classes for flexible logging to files, syslog, IDSA and other destinations.

The new **log4cpp** package contains the 1.0 version of **log4cpp** for applications that need log4j style logging capabilities.

Users of Spice and users requiring application support of the log4cpp package are advised to install this package.

2.17. RHEA-2009:1245: pdksh

A new **pdksh** package which provides a public domain implementation of the ksh-88 interactive and shell-scripting language is now available for Red Hat Enterprise Linux 5.

The Public Domain Korn SHell implements the ksh-88 programming language for both interactive and shell script use.

This new **pdksh** package provides an alternative to **ksh** (ksh-93) for backward compatibility. It is also useful in situations where customers would like to port their scripts from ksh-88 to ksh-93.

Important: the **pdksh** package can be installed alongside the ksh package on the same system, thus providing both ksh-88 and ksh-93 Korn shell implementations. The **alternatives** utility can be used to switch between them. To set or change the ksh implementation, enter the following at the shell prompt as the root user:

```
alternatives --config ksh
```

You will then be prompted for the ksh implementation you prefer to use. On systems which have the ksh package installed, ksh-93 will be the default implementation unless this is changed by using "**alternatives**", or unless the ksh package is uninstalled and the pdksh package is installed.

The "**`#!/bin/ksh`**" bang line at the top of Korn shell scripts causes the ksh implementation selected in "**alternatives**", which is ksh-93 by default, to run that script. To force scripts to run with the correct ksh implementation despite which Korn shell implementation is selected in "**alternatives**", employ the following bang lines:

for ksh-88: the first line of the script should read "#!/bin/pdksh"

for ksh-93: the first line of the script should read"#!/bin/ksh93"

All users requiring **pdksh** should install this newly-released package, which adds this enhancement.

2.18. RHEA-2009:1302: perl-Sys-Virt

A new **perl-Sys-Virt** package is now available for Red Hat Enterprise Linux 5.4 that allows libvirt to be used from Perl.

The new **perl-SyS-Virt** package provides an API for managing virtual machines from Perl, using the **libvirt** library.

This new package reflects changes made for the release of Red Hat Enterprise Linux 5.4.

Users of Red Hat Enterprise Linux 5 should upgrade to this updated package.

2.19. RHEA-2009:1293: pinentry

A new package, **pinentry**, is now available for Red Hat Enterprise Linux 5.

Pinentry is a collection of simple PIN or passphrase entry dialogs which utilize the Assuan protocol as described by the aegypten project; see http://www.gnupg.org/aegypten/ for details. The **pinentry** package also contains the curses (text) based version of the PIN entry dialog.

This new package is required by the new **gnupg2** utility. GnuPG 2.0 is a newer version of GnuPG, a tool for secure communication and data storage. GnuPG 2.0 derives from a different design philosophy and includes additional support for S/MIME. (BZ#484188)

Anyone wishing to use GnuPG 2 is advised to also install this new package.

2.20. RHEA-2009:1294: pth

A new package, **pth**, is now available for Red Hat Enterprise Linux 5.

Pth is a very portable POSIX/ANSI-C based library for Unix platforms which provides non-preemptive priority-based scheduling for multiple threads of execution ("multi-threading") inside server applications. All threads run in the same address space of the server application, but each thread has it's own individual program-counter, run-time stack, signal mask and errno variable.

This new package is required by the new gnupg2 utility. GnuPG 2.0 is a newer version of GnuPG, a tool for secure communication and data storage. GnuPG 2.0 derives from a different design philosophy and includes additional support for S/MIME. (BZ#484189)

Anyone wishing to use GnuPG 2 is advised to also install this new package.

2.21. RHEA-2009:1309: qcairo

A new package is now available for Red Hat Enterprise Linux 5.

Cairo is a 2D graphics library designed to provide high-quality display and print output. Currently supported output targets include the X Window System, OpenGL (via glitz), in-memory image buffers, and image files (PDF, PostScript, and SVG).

Cairo is designed to produce consistent output on all output media while taking advantage of display hardware acceleration when available (for example, through the X Render Extension or OpenGL).

qcairo is a version of the cairo 2D graphics library, with additional features required to support the implementation of the SPICE protocol. (BZ#488604)

Users of Red Hat Enterprise Linux 5 should install the qcairo packages for use with SPICE-enabled virtualization products.

2.22. RHBA-2009:1323: qffmpeg

A new **qffmpeg** package, required for hypervisor Spice protocol support, is now available.

qffmpeg is a stripped-down version of FFMPEG including only a limited set of the codecs available in the upstream version.

This new package provides the codecs required for SPICE protocol support in the Linux KVM hypervisor and clients. The package includes no other codecs from the upstream version, to avoid inadvertently bundling or shipping any encumbered code or binaries. (BZ#488606)

Users of Red Hat Enterprise Linux 5 should install the qffmpeg packages for use with SPICE-enabled virtualization products.

2.23. RHEA-2009:1305: qpixman

qpixman is now available as a new package for Red Hat Enterprise Linux 5.

qpixman is a pixel manipulation library for X and cairo required for SPICE protocol support. (BZ#488592)

Users of Red Hat Enterprise Linux 5 should install qpixman for use with SPICE-enabled virtualization products.

2.24. RHEA-2009:1334: qspice

A new **qspice** package 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.

Users requiring remote display capabilities for KVM hypervisors should install this new package.

2.25. RHEA-2009:1399: samba3x

A new package is now available for Red Hat Enterprise Linux 5.

Samba is a suite of programs used by machines to share files, printers, and other utilities.

samba3x contains version 3.3 of **Samba**, and is now included as a Technology Preview in Red Hat Enterprise Linux 5. To use the **samba3x** Technology Preview, the supported version of samba (provided by the **samba** package) must be removed first.

2.26. RHEA-2009:1308: xorg-x11-drv-qxl

xorg-x11-qxl-drv is a new package that is now available for Red Hat Enterprise Linux 5 as a technology preview.

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 5 as a guest operating system under KVM and QEMU, using the SPICE protocol.

Technology preview features are included in Red Hat Enterprise Linux to provide the features with wide exposure with the goal of supporting these features in a future release of Red Hat Enterprise Linux. technology preview features are not supported under Red Hat Enterprise Linux 5.4 subscription services and may not be functionally complete. Red Hat welcomes customer feedback and suggestions for technology

previews. Advisories will be provided for high-severity security issues in technology preview features.

All users who plan to preview this forthcoming technology are advised to install this new package.

2.27. RHEA-2009:1406: xorg-x11-xdm

The **xorg-x11-xdm** package is now available.

- XDM (X Window Display Manager) is a sample display manager for the X window system. This package makes XDM available in Red Hat Enterprise Linux 5 for the first time. (BZ#414171)

All users who require XDM should install this new package.

Chapter 3. Technology Previews

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

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

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

DFS

Starting with Red Hat Enterprise Linux 5.3, CIFS supports Distributed File System (DFS) as a Technology Preview.

ALUA Mode on *EMC Clariion*

Explicit active-passive failover (ALUA) mode using **`dm-multipath`** on *EMC Clariion* storage is now available. This mode is provided as per T10 specifications, but is provided in this release only as a technology preview.

For more information about T10, refer to http://www.t10.org.

ext4

The latest generation of the ext filesystem, **`ext4`**, is available in this release as a Technology Preview. **`Ext4`** is an incremental improvement on the **`ext3`** file system developed by Red Hat and the Linux community. The release name of the file system for the Technology Preview is **`ext4dev`**.

The file system is provided by the **`ext4dev.ko`** kernel module, and a new **`e4fsprogs`** package, which contains updated versions of the familiar e2fsprogs administrative tools for use with ext4. To use, install **`e4fsprogs`** and then use commands like **`mkfs.ext4dev`** from the e4fsprogs program to create an ext4-base file system. When referring to the filesystem on a mount commandline or fstab file, use the filesystem name **`ext4dev`**.

FreeIPMI

FreeIPMI is now included in this update as a Technology Preview. FreeIPMI is a collection of Intelligent Platform Management IPMI system software. It provides in-band and out-of-band software, along with a development library conforming to the Intelligent Platform Management Interface (IPMI v1.5 and v2.0) standards.

For more information about FreeIPMI, refer to http://www.gnu.org/software/freeipmi/

TrouSerS and tpm-tools

TrouSerS and **`tpm-tools`** are included in this release to enable use of *Trusted Platform Module* (TPM) hardware.TPM hardware features include (among others):

- Creation, storage, and use of RSA keys securely (without being exposed in memory)
- Verification of a platform's software state using cryptographic hashes

TrouSerS is an implementation of the Trusted Computing Group's Software Stack (TSS) specification. You can use TrouSerS to write applications that make use of TPM hardware. **tpm-tools** is a suite of tools used to manage and utilize TPM hardware.

For more information about TrouSerS, refer to http://trousers.sourceforge.net/.

eCryptfs

eCryptfs is a stacked cryptographic file system for Linux. It mounts on individual directories in existing mounted lower file systems such as EXT3; there is no need to change existing partitions or file systems in order to start using **eCryptfs**.

With this release, **eCryptfs** has been re-based to upstream version 56, which provides several bug fixes and enhancements. In addition, this update provides a graphical program to help configure **eCryptfs** (**ecryptfs-mount-helper-gui**).

This update also changes the syntax of certain **eCryptfs** mount options. If you choose to update to this version of **eCryptfs**, you should update any affected mount scripts and **/etc/fstab** entries. For information about these changes, refer to **man ecryptfs**.

The following caveats apply to this release of **eCryptfs**:

- Note that the **eCryptfs** file system will only work properly if the encrypted file system is mounted once over the underlying directory of the same name. For example:

  ```
  mount -t ecryptfs /mnt/secret /mnt/secret
  ```

  The secured portion of the file system should not be exposed, i.e. it should not be mounted to other mount points, bind mounts, and the like.

- **eCryptfs** mounts on networked file systems (e.g. NFS, Samba) will not work properly.

- This version of the **eCryptfs** kernel driver requires updated userspace, which is provided by **ecryptfs-utils-56-4.el5** or newer.

For more information about **eCryptfs**, refer to http://ecryptfs.sf.net. You can also refer to http://ecryptfs.sourceforge.net/README and http://ecryptfs.sourceforge.net/ecryptfs-faq.html for basic setup information.

Stateless Linux

Stateless Linux is a new way of thinking about how a system should be run and managed, designed to simplify provisioning and management of large numbers of systems by making them easily replaceable. This is accomplished primarily by establishing prepared system images which get replicated and managed across a large number of stateless systems, running the operating system in a read-only manner (refer to **/etc/sysconfig/readonly-root** for more details).

In its current state of development, the Stateless features are subsets of the intended goals. As such, the capability remains as Technology Preview.

Red Hat recommends that those interested in testing stateless code read the HOWTO at http://fedoraproject.org/wiki/StatelessLinux/HOWTO and join stateless-list@redhat.com.

The enabling infrastructure pieces for Stateless Linux were originally introduced in Red Hat Enterprise Linux 5.

AIGLX

AIGLX is a Technology Preview feature of the otherwise fully supported X server. It aims to enable GL-accelerated effects on a standard desktop. The project consists of the following:

GL-accelerated effects on a standard desktop. The project consists of the following:

- A lightly modified X server.
- An updated Mesa package that adds new protocol support.

By installing these components, you can have GL-accelerated effects on your desktop with very few changes, as well as the ability to enable and disable them at will without replacing your X server. AIGLX also enables remote GLX applications to take advantage of hardware GLX acceleration.

FireWire

The **`firewire-sbp2`** module is still included in this update as a Technology Preview. This module enables connectivity with FireWire storage devices and scanners.

At present, FireWire does not support the following:

- IPv4
- *pcilynx* host controllers
- multi-LUN storage devices
- non-exclusive access to storage devices

In addition, the following issues still exist in FireWire:

- a memory leak in the **SBP2** driver may cause the machine to become unresponsive.
- a code in this version does not work properly in big-endian machines. This could lead to unexpected behavior in PowerPC.

ktune

This release includes **`ktune`** (from the **`ktune`** package), a service that sets several kernel tuning parameters to values suitable for specific system profiles. Currently, **`ktune`** only provides a profile for large-memory systems running disk-intensive and network-intensive applications.

The settings provides by **`ktune`** do not override those set in **`/etc/sysctl.conf`** or through the kernel command line. **`ktune`** may not be suitable on some systems and workloads; as such, you should test it comprehensively before deploying to production.

You can disable any configuration set by **`ktune`** and revert to your normall settings by simply stopping the **`ktune`** service using **`service ktune stop`** (as root).

SGPIO Support for dmraid

Serial General Purpose Input Output (SGPIO) is an industry standard communication method used between a main board and a variety of internal and external hard disk drive bay enclosures. This method can be used to control LED lights on an enclosure through the AHCI driver interface.

In this release, SGPIO support in **dmraid** is included as a technology preview. This will allow **dmraid** to work properly with disk enclosures.

GCC 4.4

The *Gnu Compiler Collection version 4.4 (GCC4.4)* is now included in this release as a Technology Preview. This collection of compilers include C, C++, and Fortran compilers along with support libraries.

Note that in the **gcc44** packages, the default for the **gnu89-inline** option has been changed to **-fgnu89-inline**, whereas upstream and future updates of Red Hat Enterprise Linux 5 will default to **-fno-gnu89-inline**. This is necessary because many headers shipped as part of Red Hat Enterprise Linux 5 expect GNU in-line semantics instead of ISO C99 semantics. These headers have not been adjusted to request GNU in-line semantics through attributes.

Kernel Tracepoint Facility

In this update, a new kernel marker/tracepoint facility has been implemented as a Technology Preview. This interface adds static probe points into the kernel, for use with tools such as **SystemTap**.

Device Failure Monitoring of RAID sets

Device Failure Monitoring, using the tools dmraid and dmevent_tool, is included in Red Hat Enterprise Linux 5.3 as a Technology Preview. This provides the ability to watch and report device failures on component devices of RAID sets.

Software based Fibre Channel over Ethernet (FCoE)

The Fibre Channel over Ethernet (FCoE) driver (fcoe.ko), along with libfc, provides the ability to run FCoE over a standard Ethernet card. This capability is provided as a technical preview in Red Hat Enterprise Linux 5.3.

To enable this feature, you must login by writing the network interface name to the **/sys/module/fcoe/parameters/create** file, for example:

```
echo eth6 > /sys/module/fcoe/parameters/create
```

To logout, write the network interface name to the **/sys/module/fcoe/parameters/destroy** file, for example:

```
echo eth6 > /sys/module/fcoe/parameters/destroy
```

For further information on software based FCoE refer to: http://www.open-fcoe.org/openfc/wiki/index.php/FCoE_Initiator_Quickstart.

Red Hat Enterprise Linux 5.3 provides full support for FCoE on three specialized hardware implementations. These are: Cisco **fnic** driver, the Emulex **lpfc** driver, and the Qlogic **qla2xx** driver.

iSER Support

iSER support, allowing for block storage transfer across a network, has been added to the **scsi-target-utils** package as a Technology Preview. In this release, single portal and multiple portals on different subnets are supported. There are known bugs when using multiple portals on the same subnet.

To set up the iSER target component install the scsi-target-utils and libibverbs-devel RPM. The library package for the InfiniBand hardware that is being used is also required. For example: host channel adapters that use the **cxgb3** driver the **libcxgb3** package is needed, and for host channel adapters using the **mthca** driver the **libmthca** package is needed.

There is also a known issue relating to connection timeouts in some situations. Refer to Red Hat Bugzilla #470627 for more information on this issue.

iSER Support

iSER support, allowing for block storage transfer across a network, has been added to the **scsi-target-utils** package as a Technology Preview. In this release, single portal and multiple portals on different subnets are supported. There are known bugs when using multiple portals on the same subnet.

To set up the iSER target component install the scsi-target-utils and libibverbs-devel RPM. The library package for the InfiniBand hardware that is being used is also required. For example: host channel adapters that use the **cxgb3** driver the **libcxgb3** package is needed, and for host channel adapters using the **mthca** driver the **libmthca** package is needed.

There is also a known issue relating to connection timeouts in some situations. Refer to Red Hat Bugzilla #470627 for more information on this issue.

cman fence_virsh fence agent

The fence_virsh fence agent is provided in this release of Red Hat Enterprise Linux as a Technology Preview. fence_virsh provides the ability for one guest (running as a domU) to fence another using the libvirt protocol. However, as fence_virsh is not integrated with cluster-suite it is not supported as a fence agent in that environment.

glibc new MALLOC behaviour

The upstream glibc has been changed recently to enable higher scalability across many sockets and cores. This is done by assigning threads their own memory pools and by avoiding locking in some situations. The amount of additional memory used for the memory pools (if any) can be controlled using the environment variables MALLOC_ARENA_TEST and MALLOC_ARENA_MAX.

MALLOC_ARENA_TEST specifies that a test for the number of cores is performed once the number of memory pools reaches this value. MALLOC_ARENA_MAX sets the maximum number of memory pools used, regardless of the number of cores.

The glibc in the RHEL 5.4 release has this functionality integrated as a Technology Preview of the upstream malloc. To enable the per-thread memory pools the environment variable MALLOC_PER_THREAD needs to be set in the environment. This environment variable will become obsolete when this new malloc behaviour becomes default in future releases. Users experiencing contention for the malloc resources could try enabling this option.

Chapter 4. Known Issues

4.1. anaconda

The anaconda package contains the program which was used to install your system.

The following are the Known Issues that apply to the anaconda package in Red Hat Enterprise Linux 5.4

- When installing to an ext3 or ext4 file system, anaconda disables periodic filesystem checking. Unlike ext2, these filesystems are journaled, removing the need for a periodic filesystem check. In the rare cases where there is an error detected at runtime or an error while recovering the filesystem journal, the file system check will be run at boot time. (BZ#513480)

- When installing KVM or Xen guests, always create a partition for the guest disk, or create an LVM volume. Guests should not be installed to block devices or raw disk devices. Anaconda includes disk label duplication avoidance code, but when installing within a VM, it has no visibility to the disk labels elsewhere on the host and cannot detect duplicates.

  If guest filesystems, especially the root filesystem, are directly visible to the host, a host OS reboot may inadvertantly parse the partition table and mount the guest filesystems. This can lead to highly undesirable outcomes. (BZ#518461)

- The minimum memory requirement when installing all Red Hat Enterprise Linux packages (i.e. '*' or '@everything' is listed in the %packages section of the kickstart file) on a fully virtualized Itanium guest is 768MB. After installation, the memory allocated to the guest can be lowered to the desired amount. (BZ#507891)

- Upgrading a system using Anaconda is not possible if the system is installed on disks attached using zFCP or iSCSI (unless booted from the disk using a network adaptor with iBFT). Such disks are activated after Anaconda scans for upgradable installations and are not found. To update please use the Red Hat Network with the hosted Web user interface, a Red Hat Network Satellite, the local graphical Updater, or the yum command line. (BZ#494033)

- Anaconda's graphical installer fails to start at the default 800x600 resolution on systems utilizing Intel Graphics Device Next Generation (IGDNG) devices. To work around this issue, ensure anaconda uses a higher resolution by passing the parameters **`resolution=1024x768`** or **`resolution=1280x1024`**" to the installer using the boot command line.

- The NFS default for RHEL5 is "locking". Therefore, to mount nfs shares from the %post section of anaconda, use the **`mount -o nolock,udp`** command to start the locking daemon before using nfs to mount shares. (BZ#426053)

- If you are using the Virtualized kernel when upgrading from Red Hat Enterprise Linux 5 to 5.2, you must reboot after completing the upgrade. You should then boot the system using the updated Virtualized kernel.

  The hypervisors of Red Hat Enterprise Linux 5 and 5.2 are not ABI-compatible. If you do not boot the system after upgrading using the updated Virtualized kernel, the upgraded Virtualization RPMs will not match the running kernel. (BZ#251669)

- When upgrading to Red Hat Enterprise Linux 5.1 or later from Red Hat Enterprise Linux 4.6, **`gcc4`** may cause the upgrade to fail. As such, you should manually remove the **`gcc4`** package before upgrading. (BZ#432773)

- When provisioning guests during installation, the **RHN tools for guests** option will not be available. When this occurs, the system will require an additional entitlement, separate from the entitlement used by **`dom0`**.

To prevent the consumption of additional entitlements for guests, install the **rhn-virtualization-common** package manually before attempting to register the system to Red Hat Network. (BZ#431648)

- When installing Red Hat Enterprise Linux 5 on a guest, the guest is configured to explicitly use a temporary installation kernel provided by **dom0**. Once installation finishes, it can then use its own bootloader. However, this can only be achieved by forcing the guest's first reboot to be a shutdown.

  As such, when the **Reboot** button appears at the end of the guest installation, clicking it shuts down the guest, but does not reboot it. This is an expected behavior.

  Note that when you boot the guest after this it will then use its own bootloader. (BZ#328471)

- Using the **swap --grow** parameter in a kickstart file without setting the **--maxsize** parameter at the same time makes anaconda impose a restriction on the maximum size of the swap partition. It does not allow it to grow to fill the device.

  For systems with less than 2GB of physical memory, the imposed limit is twice the amount of physical memory. For systems with more than 2GB, the imposed limit is the size of physical memory plus 2GB. (BZ#462734)

- Existing encrypted block devices that contain **vfat** file systems will appear as type **foreign** in the partitioning interface; as such, these devices will not be mounted automatically during system boot. To ensure that such devices are mounted automatically, add an appropriate entry for them to **/etc/fstab**. For details on how to do so, refer to **man fstab**. (BZ#467202)

- when using anaconda's automatic partitioning on an IBM System p partition with multiple harddisks containing different Linux distributions, the anaconda installer may overwrite the bootloaders of the other Linux installations although their harddisks have been unchecked. To work around this, choose manual partitioning during the installation process.(BZ#519795)

The following note applies to PowerPC Architectures:

- The minimum RAM required to install Red Hat Enterprise Linux 5.2 is 1GB; the recommended RAM is 2GB. If a machine has less than 1GB RAM, the installation process may hang.

  Further, PowerPC-based machines that have only 1GB of RAM experience significant performance issues under certain RAM-intensive workloads. For a Red Hat Enterprise Linux 5.2 system to perform RAM-intensive processes optimally, 4GB of RAM is recommended. This ensures the system has the same number of physical pages as was available on PowerPC machines with 512MB of RAM running Red Hat Enterprise Linux 4.5 or earlier. (BZ#209165)

The following note applies to s390x Architectures:

- Installation on a machine with existing Linux or non-Linux filesystems on DASD block devices may cause the installer to halt. If this happens, it is necessary to clear out all existing partitions on the DASD devices you want to use and restart the installer. (BZ#289631)

The following note applies to the ia64 Architecture:

- If your system only has 512MB of RAM, attempting to install Red Hat Enterprise Linux 5.4 may fail. To prevent this, perform a base installation first and install all other packages after the installation finishes. (BZ#435271)

4.2. cmirror

The cmirror packages provide user-level utilities for managing cluster mirroring.

- Due to limitations in the cluster infrastructure, cluster mirrors greater than 1.5TB cannot be created with the default region size. If larger mirrors are required, the region size should be increased from its default (512kB), for example:

```
# -R <region_size_in_MiB>
lvcreate -m1 -L 2T -R 2 -n mirror vol_group
```

  Failure to increase the region size will result in the LVM creation process hanging and may cause other LVM commands to hang. (BZ#514814)

4.3. compiz

Compiz is an OpenGL-based window and compositing manager.

- Running **rpmbuild** on the **compiz** source RPM will fail if any KDE or **qt** development packages (for example, **qt-devel**) are installed. This is caused by a bug in the **compiz** configuration script.

  To work around this, remove any KDE or **qt** development packages before attempting to build the **compiz** package from its source RPM. (BZ#444609)

4.4. device-mapper-multipath

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

- When using **dm-multipath**, if **features "1 queue_if_no_path"** is specified in **/etc/multipath.conf** then any process that issues I/O will hang until one or more paths are restored.

  To avoid this, set **no_path_retry *[N]*** in **/etc/multipath.conf** (where ***[N]*** is the number of times the system should retry a path). When you do, remove the **features "1 queue_if_no_path"** option from **/etc/multipath.conf** as well.

  If you need to use **"1 queue_if_no_path"** and experience the issue noted here, use **dmsetup** to edit the policy at runtime for a particular LUN (i.e. for which all the paths are unavailable).

  To illustrate: run **dmsetup message *[device]* 0 "fail_if_no_path"**, where ***[device]*** is the multipath device name (e.g. **mpath2**; do not specify the path) for which you want to change the policy from **"queue_if_no_path"** to **"fail_if_no_path"**. (BZ#419581)

- When a LUN is deleted on a configured storage system, the change is not reflected on the host. In such cases, **lvm** commands will hang indefinitely when **dm-multipath** is used, as the LUN has now become *stale*.

  To work around this, delete all device and **mpath** link entries in **/etc/lvm/.cache** specific to the stale LUN.

  To find out what these entries are, run the following command:

  ls -l /dev/mpath | grep *[stale LUN]*

  For example, if ***[stale LUN]*** is 3600d0230003414f30000203a7bc41a00, the following results may appear:

```
lrwxrwxrwx 1 root root 7 Aug  2 10:33 /3600d0230003414f30000203a7bc41a00 -
> ../dm-4
lrwxrwxrwx 1 root root 7 Aug  2 10:33 /3600d0230003414f30000203a7bc41a00p1
-> ../dm-5
```

This means that 3600d0230003414f30000203a7bc41a00 is mapped to two **mpath** links: **dm-4** and **dm-5**.

As such, the following lines should be deleted from **/etc/lvm/.cache**:

```
/dev/dm-4
/dev/dm-5
/dev/mapper/3600d0230003414f30000203a7bc41a00
/dev/mapper/3600d0230003414f30000203a7bc41a00p1
/dev/mpath/3600d0230003414f30000203a7bc41a00
/dev/mpath/3600d0230003414f30000203a7bc41a00p1
```

(BZ#238421)

- Running the **multipath** command with the **-ll** option can cause the command to hang if one of the paths is on a blocking device. Note that the driver does not fail a request after some time if the device does not respond.

  This is caused by the cleanup code, which waits until the path checker request either completes or fails. To display the current **multipath** state without hanging the command, use **multipath -l** instead. (BZ#214838)

4.5. dmraid

The dmraid packages contain the ATARAID/DDF1 activation tool that supports RAID device discovery, RAID set activation, and displays properties for ATARAID/DDF1 formatted RAID sets on Linux kernels using device-mapper.

- The **/etc/cron.d/dmeventd-logwatch** crontab file does not specify the user that the logwatch process should be executed by. To work around this issue, the functional portion of this crontab must be changed to:

  ```
  * * * * * root /usr/sbin/logwatch --service dmeventd --range today --
  detail med
  ```

  (BZ#516892)

- The installation procedure stores the name of RAID volume and partition in an initscript. When the system boots, dmraid enables the RAID partition (that are named implicitly in the init script. This action functions until the volume and partition names are changed. In these cases, the system may not boot, and the user is given an option to reboot system and start the rebuild procedure in OROM.

  OROM changes the name of RAID volume (as seen by dmraid) and dmraid cannot recognize the array identified by previous name stored in initscript. The system no longer boots from RAID partition, since it is not enabled by dmraid. In case of RAID 1 (mirror), the system may be booted from disk that is part of RAID volume. However, dmraid does not allow to active or rebuild the volume which component in mounted.

To work around this issue, do not rebuild the RAID array in OROM. Start the rebuild procedure by dmraid in the operating system, which performs all the steps of rebuilding. dmraid does not change the RAID volume name, therefore the system can be booted from RAID array without the need of init script modification.

To modify init script after OROM has started rebuild:

- Start the system in rescue mode from the installation disk, skip finding and mounting previous installations.
- At the command line, find and enable the raid volume that is to be booted from (the RAID volume and partitions will be activated)

```
dmraid -ay isw_effjffhbi_Volume0
```

- Mount the root partition:

```
mkdir /tmp/raid
mount /dev/mapper/isw_effjffhbi_Volume0p1 /tmp/raid
```

- Decompress the boot image:

```
mkdir /tmp/raid/tmp/image
cd /tmp/raid/tmp/image
gzip -cd /tmp/raid/boot/inird-2.6.18-155.el5.img | cpio -imd –quiet
```

- Change the names of the RAID volumes in the initscript to use the new names of RAID:

```
dmraid –ay –I –p –rm_partition “/dev/mapper/isw_effjffhbi_Volume0”
kpartx –a –p p “/dev/mapper/isw_effjffhbi_Volume0”
mkrtootdev –t ext3 –o defaults,ro
/dev/mapper/isw_effjffhbi_Volume0p1
```

- compress and copy initrd image with the modified init script to the boot directory

```
cd /tmp/raid/tmp/image
find . –print | cpio –c –o | gzip -9 > /tmp/raid/boot/inird-2.6.18-
155.el5.img
```

- unmount the raid volume and reboot the system:

```
umount /dev/mapper/isw_effjffhbi_Volume0p1
dmraid -an
```

4.6. dogtail

dogtail is a GUI test tool and automation framework that uses assistive technologies to communicate with desktop applications.

- Attempting to run **`sniff`** may result in an error. This is because some required packages are not installed with **`dogtail`**. (BZ#435702)

To prevent this from occurring, install the following packages manually:

- librsvg2
- ghostscript-fonts
- pygtk2-libglade

4.7. firstboot

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

The following notes apply to s390x Architectures:

- The *IBM System z* does not provide a traditional Unix-style physical console. As such, Red Hat Enterprise Linux 5.2 for the *IBM System z* does not support the *firstboot* functionality during initial program load.

  To properly initialize setup for Red Hat Enterprise Linux 5.2 on the *IBM System z*, run the following commands after installation:

  - **`/usr/bin/setup`** — provided by the **`setuptool`** package.
  - **`/usr/bin/rhn_register`** — provided by the **`rhn-setup`** package.

  (BZ#217921)

4.8. gfs2-utils

The gfs2-utils packages provide the user-level tools necessary to mount, create, maintain and test GFS2 file systems.

If gfs2 is used as the root file system, the first boot attempt will fail with the error message "**`fsck.gfs2: invalid option -- a`**". To work around this issue:

1. Enter the root password when prompted
2. Mount the root file system manually:

   ```
   mount -o remount,rw /dev/VolGroup00/LogVol00 /
   ```

3. Edit the /etc/fstab file from:

   ```
   /dev/VolGroup00/LogVol00 / gfs2 defaults 1 1
   ```

   to

   ```
   /dev/VolGroup00/LogVol00 / gfs2 defaults 1 0
   ```

4. Reboot the system.

4.9. gnome-volume-manager

The GNOME Volume Manager monitors volume-related events and responds with user-specified policy. The GNOME Volume Manager can automount hot-plugged drives, automount inserted removable media, autorun programs, automatically play audio CDs and video DVDs, and automatically import photos from a digital camera.

- Removable storage devices (such as CDs and DVDs) do not automatically mount when you are logged in as root. As such, you will need to manually mount the device through the graphical file manager. (BZ#209362)

  Alternatively, you can run the following command to mount a device to **/media**:

  ```
  mount /dev/[device name] /media
  ```

4.10. initscripts

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

- On systems with more than two encrypted block devices, anaconda has a option to provide a global passphrase. The init scripts, however, do not support this feature. When booting the system, entering each individual passphrase for all encrypted devices will be required. (BZ#464895)
- Boot-time logging to **/var/log/boot.log** is not available in Red Hat Enterprise Linux 5.3. (BZ#223446, BZ#210136)

4.11. iscsi-initiator-utils

The iscsi package provides the server daemon for the 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.

- Removing the **bnx2** modules or running ifdown on the network interface being used by **bnx2i** driver will result in the iSCSI sessions being disconnected. Reloading the module or running ifup, will not reconnect the SCSI sessions. To work around this issue, the iscsi service must be stopped and then restarted. (BZ#514926)
- iSCSI iface binding is not supported during install or boot. The initiator only supports the ability to log into target portals using the default behavior where the initiator uses the network routing table to decide which NIC to use.

  To work around this limitation, booting or installation can be done using the default behavior. After the iscs and iscsid services start, the iscsi service can log into the target using iSCSI iface binding. This however, will leave an extra session using the default behavior, and it has to be manually logged out using the following command:

  ```
  iscsiadm -m node -T target -p ip -I default -u
  ```

  (BZ#500273)

4.12. kernel-xen

- When booting paravirtualized guests that support gigabyte page tables (i.e. a Fedora 11 guest) on Red Hat Enterprise Linux 5.4 Xen, the domain may fail to start if more than 2047MB of memory is configured for the domain. To work around this issue, pass the "**nogbpages**" parameter on the guest kernel command-line. (BZ#502826)

- Boot parameters are required to enable SR/IOV Virtual Function devices. SR/IOV Virtual Function devices can only be accessed if the parameter pci_pt_e820_access=on is added to the boot stanza in the /boot/grub/grub.conf file. For example:

  ```
  title Red Hat Enterprise Linux Server (2.6.18-152.el5xen)
          root (hd0,1)
          kernel /xen.gz-2.6.18-152.el5 com1=115200,8n1 console=com1
  iommu=1
          module /vmlinuz-2.6.18-152.el5xen ro root=LABEL=/
  console=ttyS0,115200
  pci_pt_e820_access=on
  ```

  This enables the MMCONF access method for the PCI configuration space, a requirement for VF device support

- When using Single Root I/O Virtualization (SR-IOV) devices under Xen, a single Hardware Virtual Machine (HVM) guest is limited to 12 Virtual Function (VF) assignments. (BZ#511403)

- When booting a fully virtualized Xen guest, the following message may be displayed on the guest console:

  ```
  testing NMI watchdog ... <4>
  WARNING: CPU#0: NMI appears to be stuck (0->0)!
  ```

  This issue is caused by an implementation issue with the Xen hypervisor and can be safely ignored. (BZ#500845)

- Diskette drive media will not be accessible when using the virtualized kernel. To work around this, use a USB-attached diskette drive instead.

  Note that diskette drive media works well with other non-virtualized kernels. (BZ#401081)

- Formatting a disk when running **Windows 2008** or **Windows Vista** as a guest can crash when the guest has been booted with multiple virtual CPUs. To work around this, boot the guest with a single virtual CPU when formatting. (BZ#441627)

- Fully virtualized guests cannot correct for time lost due to the domain being paused and unpaused. Being able to correctly track the time across pause and unpause events is one of the advantages of paravirtualized kernels. This issue is being addressed upstream with replaceable timers, so fully virtualized guests will have paravirtualized timers. Currently, this code is under development upstream and should be available in later versions of Red Hat Enterprise Linux. (BZ#422531)

The following note applies to x86_64 Architectures:

- Upgrading a host (**dom0**) system to Red Hat Enterprise Linux 5.2 may render existing Red Hat Enterprise Linux 4.5 SMP paravirtualized guests unbootable. This is more likely to occur when the host system has more than 4GB of RAM.

  To work around this, boot each Red Hat Enterprise Linux 4.5 guest in single CPU mode and upgrade its kernel to the latest version (for Red Hat Enterprise Linux 4.5.z). (BZ#253087, BZ#251013)

The following note applies to the ia64 Architecture:

- On some *Itanium* systems configured for console output to VGA, the **dom0** virtualized kernel may fail to boot. This is because the virtualized kernel failed to properly detect the default console device from the *Extensible Firmware Interface* (EFI) settings.

  When this occurs, add the boot parameter **console=tty** to the kernel boot options in **/boot/efi/elilo.conf**. (BZ#249076)

- On some *Itanium* systems (such as the *Hitachi Cold Fusion 3e*), the serial port cannot be detected in **dom0** when VGA is enabled by the EFI Maintenance Manager. As such, you need to supply the following serial port information to the **dom0** kernel:

  - Speed in bits/second
  - Number of data bits
  - Parity
  - **io_base** address

  These details must be specified in the **append=** line of the **dom0** kernel in **/boot/efi/elilo.conf**. For example:

  append="com1=19200,8n1,0x3f8 -- quiet rhgb console=tty0 console=ttyS0,19200n8"

  In this example, **com1** is the serial port, **19200** is the speed (in bits/second), **8n1** specifies the number of data bits/parity settings, and **0x3f8** is the **io_base** address. (BZ#433771)

- Virtualization does not work on some architectures that use Non-Uniform Memory Access (NUMA). As such, installing the virtualized kernel on systems that use NUMA will result in a boot failure.

  Some installation numbers install the virtualized kernel by default. If you have such an installation number and your system uses NUMA and does not work with kernel-xen, deselect the Virtualization option during installation. (BZ#293071)

4.13. kernel

The Kernel

- Under some circumstances, the sky2 driver may hang, returning the following error message:

  ```
  sky2 eth<N>: receiver hang detected
  ```

  Currently, the only work around to make the device online again is to reboot the system. This bug will be repaired in an upcoming update to Red Hat Enterprise Linux 5.4. (BZ#509891, BZ#517976)

- On certain hardware configurations the kernel may panic when the Broadcom iSCSI offload driver (**bnx2i.ko** and **cnic.ko**) is loaded. To work around this do not manually load the bnx2i or cnic modules, and temporarily disable the **iscsi** service from starting. To disable the iscsi service, run

  ```
  chkconfig --del iscsi
  chkconfig --del iscsid
  ```

  On the first boot of your system, the **iscsi** service may start automatically. To bypass this, during bootup, enter interactive start up and stop the iscsi service from starting.

- In Red Hat Enterprise Linux 5, invoking the kernel system call "setpriority()" with a "which" parameter of type "PRIO_PROCESS" does not set the priority of child threads. (BZ#472251)

- Physical CPUs cannot be safely placed offline or online when the 'kvm_intel' or 'kvm_amd' module is loaded. This precludes physical CPU offline and online operations when KVM guests that utilize processor virtualization support are running. It also precludes physical CPU offline and online operations without KVM guests running when the 'kvm_intel' or 'kvm_amd' module is simply loaded and not being used.

  If the kmod-kvm package is installed, the 'kvm_intel' or 'kvm_amd' module automatically loads during boot on some systems. If a physical CPU is placed offline while the 'kvm_intel' or 'kvm_amd' module is loaded a subsequent attempt to online that CPU may fail with an I/O error.

  To work around this issue, unload the 'kvm_intel' or 'kvm_amd' before performing physical CPU hot-plug operations. It may be necessary to shut down KVM guests before the 'kvm_intel' or 'kvm_amd' will successfully unload.

  For example, to offline a physical CPU 6 on an Intel based system:

  ```
  # rmmod kvm_intel
  # echo 0 > /sys/devices/system/cpu/cpu6/online
  # modprobe kvm_intel
  ```

  (BZ#515557)

- A change to the cciss driver in Red Hat Enterprise Linux 5.4 made it incompatible with the "echo disk > /sys/power/state" suspend-to-disk operation. Consequently, the system will not suspend properly, returning messages such as:

  ```
  Stopping tasks:
  ======================================================================
   stopping tasks timed out after 20 seconds (1 tasks remaining):
    cciss_scan00
  Restarting tasks...<6> Strange, cciss_scan00 not stopped
   done
  ```

  (BZ#513472)

- The kernel is unable to properly detect whether there is media present in a CD-ROM drive during kickstart installs. The function to check the presence of media incorrectly interprets the "logical unit is becoming ready" sense, returning that the drive is ready when it is not. To work around this issue, wait several seconds between inserting a CD and asking the installer (anaconda) to refresh the CD. (BZ#510632)

- When a cciss device is under high I/O load, the kdump kernel may panic and the vmcore dump may not be saved successfully. (BZ#509790)

- Applications attempting to **`malloc`** memory approximately larger than the size of the physical memory on the node on a NUMA system may hang or appear to stall. This issue may occur on a NUMA system where the remote memory distance, as defined in SLIT, is greater than 20 and RAM based filesystem like **`tmpfs`** or **`ramfs`** is mounted.

  To work around this issue, unmount all RAM based filesystems (i.e. tmpfs or ramfs). If unmounting the RAM based filesystems is not possible, modify the application to allocate lesser memory. Finally, if modifying the application is not possible, disable NUMA memory reclaim by running:

  ```
  sysctl vm.zone_reclaim_mode=0
  ```

Important

Turning NUMA reclaim negatively effects the overall throughput of the system.

(BZ#507360)

- Configuring IRQ SMP affinity has no effect on some devices that use message signalled interrupts (MSI) with no MSI per-vector masking capability. Examples of such devices include *Broadcom NetXtreme* Ethernet devices that use the **bnx2** driver.

  If you need to configure IRQ affinity for such a device, disable MSI by creating a file in **/etc/modprobe.d/** containing the following line:

  ```
  options bnx2 disable_msi=1
  ```

  Alternatively, you can disable MSI completely using the kernel boot parameter **pci=nomsi**. (BZ#432451)

- The **smartctl** tool cannot properly read SMART parameters from SATA devices. (BZ#429606)

- *IBM T60* laptops will power off completely when suspended and plugged into a docking station. To avoid this, boot the system with the argument **acpi_sleep=s3_bios**. (BZ#439006)

- The *QLogic iSCSI Expansion Card* for the *IBM Bladecenter* provides both ethernet and iSCSI functions. Some parts on the card are shared by both functions. However, the current **qla3xxx** and **qla4xxx** drivers support ethernet and iSCSI functions individually. Both drivers do not support the use of ethernet and iSCSI functions simultaneously.

  Because of this limitation, successive resets (via consecutive **ifdown**/**ifup** commands) may hang the device. To avoid this, allow a 10-second interval after an **ifup** before issuing an **ifdown**. Also, allow the same 10-second interval after an **ifdown** before issuing an **ifup**. This interval allows ample time to stabilize and re-initialize all functions when an **ifup** is issued. (BZ#276891)

- Laptops equipped with the *Cisco Aironet MPI-350* wireless may hang trying to get a DHCP address during any network-based installation using the wired ethernet port.

  To work around this, use local media for your installation. Alternatively, you can disable the wireless card in the laptop BIOS prior to installation (you can re-enable the wireless card after completing the installation). (BZ#213262)

- Hardware testing for the *Mellanox MT25204* has revealed that an internal error occurs under certain high-load conditions. When the **ib_mthca** driver reports a catastrophic error on this hardware, it is usually related to an insufficient completion queue depth relative to the number of outstanding work requests generated by the user application.

  Although the driver will reset the hardware and recover from such an event, all existing connections at the time of the error will be lost. This generally results in a segmentation fault in the user application. Further, if **opensm** is running at the time the error occurs, then you need to manually restart it in order to resume proper operation. (BZ#251934)

- The *IBM T41* laptop model does not enter **Suspend Mode** properly; as such, **Suspend Mode** will still consume battery life as normal. This is because Red Hat Enterprise Linux 5 does not yet include the **radeonfb** module.

  To work around this, add a script named **hal-system-power-suspend** to **/usr/share/hal/scripts/** containing the following lines:

```
chvt 1
radeontool light off
radeontool dac off
```

This script will ensure that the *IBM T41* laptop enters **Suspend Mode** properly. To ensure that the system resumes normal operations properly, add the script **`restore-after-standby`** to the same directory as well, containing the following lines:

```
radeontool dac on
radeontool light on
chvt 7
```

(BZ#227496)

- If the **edac** module is loaded, BIOS memory reporting will not work. This is because the **edac** module clears the register that the BIOS uses for reporting memory errors.

  The current Red Hat Enterprise Linux Driver Update Model instructs the kernel to load all available modules (including the **edac** module) by default. If you wish to ensure BIOS memory reporting on your system, you need to manually blacklist the **edac** modules. To do so, add the following lines to **`/etc/modprobe.conf`**:

```
blacklist edac_mc
blacklist i5000_edac
blacklist i3000_edac
blacklist e752x_edac
```

  (BZ#441329)

- Due to outstanding driver issues with hardware encryption acceleration, users of Intel WiFi Link 4965, 5100, 5150, 5300, and 5350 wireless cards are advised to disable hardware accelerated encryption using module parameters. Failure to do so may result in the inability to connect to Wired Equivalent Privacy (WEP) protected wireless networks after connecting to WiFi Protected Access (WPA) protected wireless networks.

  To do so, add the following options to **`/etc/modprobe.conf`**:

```
alias wlan0 iwlagn
options iwlagn swcrypto50=1 swcrypto=1
```

  (where wlan0 is the default interface name of the first Intel WiFi Link device)

  (BZ#468967)

The following note applies to PowerPC Architectures:

- The size of the PPC kernel image is too large for OpenFirmware to support. Consequently, network booting will fail, resulting in the following error message:

```
Please wait, loading kernel...
/pci@8000000f8000000/ide@4,1/disk@0:2,vmlinux-anaconda: No such file or
directory
boot:
```

To work around this:

- Boot to the OpenFirmware prompt, by pressing the '8' key when the IBM splash screen is displayed.
- Run the following command:

  ```
  setenv real-base 2000000
  ```

- Boot into System Managment Services (SMS) with the command:

  ```
  0> dev /packages/gui obe
  ```

(BZ#462663)

4.14. kexec-tools

kexec-tools provides the /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature

- Executing **kdump** on an *IBM Bladecenter QS21* or *QS22* configured with NFS root will fail. To avoid this, specify an NFS dump target in **/etc/kdump.conf**. (BZ#368981)
- Some **forcedeth** based devices may encounter difficulty accessing memory above 4GB during operation in a **kdump** kernel. To work around this issue, add the following line to the **/etc/sysconfig/kdump** file:

  ```
  KDUMP_COMMANDLINE_APPEND="dma_64bit=0"
  ```

  This work around prevents the forcedeth network driver from using high memory resources in the kdump kernel, allowing the network to function properly.
- The system may not successfully reboot into a **kexec**/**kdump** kernel if X is running and using a driver other than *vesa*. This problem only exists with *ATI Rage XL* graphics chipsets.

  If X is running on a system equipped with *ATI Rage XL*, ensure that it is using the *vesa* driver in order to successfully reboot into a **kexec**/**kdump** kernel. (BZ#221656)
- **kdump** now serializes drive creation registration with the rest of the **kdump** process. Consequently, **kdump** may hang waiting for IDE drives to be initialized. In these cases, it is recommended that IDE disks not be used with **kdump**. (BZ#473852)
- It is possible in rare circumstances, for **makedumpfile** to produce erroneous results but not have them reported. This is due to the fact that **makedumpfile** processes its output data through a pipeline consisting of several stages. If **makedumpfile** fails, the other stages will still succeed, effectively masking the failure. Should a vmcore appear corrupt, and makedumpfile is in use, it is recommended that the core be recorded without makedumpfile and a bug be reported. (BZ#475487)
- kdump now restarts when CPUs or DIMMs are hot-added to a system. If multiple items are added at the

same time, several sequential restarts may be encountered. This behavior is intentional, as it minimizes the time-frame where a crash may occur while memory or processors are not being tracked by kdump. (BZ#474409)

The following note applies to ia64 Architecture:

- Some *Itanium* systems cannot properly produce console output from the **kexec purgatory** code. This code contains instructions for backing up the first 640k of memory after a crash.

  While **purgatory** console output can be useful in diagnosing problems, it is not needed for **kdump** to properly function. As such, if your *Itanium* system resets during a **kdump** operation, disable console output in **purgatory** by adding **--noio** to the **KEXEC_ARGS** variable in **/etc/sysconfig/kdump**. (BZ#436426)

4.15. krb5

Kerberos 5 is a network authentication system which authenticates clients and servers to each other using symmetric key encryption and a trusted third party, the KDC.

- The format of a stash file, while not architecture-specific, is endian-specific. Consequently, a stash file is not directly portable between big-endian and little-endian systems. When setting up a secondary KDC where the endianness differs from that of the master KDC, the stash file should be recreated by running '**kdb5_util create -s**' on the secondary and supplying the original master password. (BZ#514741)

4.16. kvm

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on x86 hardware.

KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems. KVM is a hypervisor which uses the libvirt virtualization tools (virt-manager and virsh).

- By default, KVM virtual machines created in Red Hat Enterprise Linux 5.4 have a virtual Realtek 8139 (rtl8139) network interface controller (NIC). The rtl8139 virtual NIC works fine in most environments, but may suffer from performance degradation issues on some networks for example, a 10 GigE (10 Gigabit Ethernet) network.

  One workaround for this issue is switch to a different type of virtual NIC, for example, Intel PRO/1000 (e1000) or virtio (a virtual I/O driver for Linux that can talk to the hypervisor).

  To switch to e1000:

  - Shutdown the guest OS
  - Edit the guest OS definition with the command-line tool virsh:

    ```
    virsh edit GUEST
    ```

  - Locate the network interface section and add a model line as shown:

    ```
    <interface type='network'>
     ...
     <model type='e1000' />
    </interface>
    ```

- Save the changes and exit the text editor
- Restart the guest OS

Alternatively, if you're having trouble installing the OS on the virtual machine because of the rtl8139 NIC (for example, because you're installing the OS over the network), you can create a virtual machine from scratch with an e1000 NIC. This method requires you to have at least one virtual machine already created (possibly installed from CD or DVD) to use as a template.

- Create an XML template from an existing virtual machine:

```
virsh dumpxml GUEST > /tmp/guest.xml
```

- Copy and edit the XML file and update the unique fields: virtual machine name, UUID, disk image, MAC address, etc. NOTE: you can delete the UUID and MAC address lines and virsh will generate a UUID and MAC address.

```
cp /tmp/guest.xml /tmp/new-guest.xml
vi /tmp/new-guest.xml
```

- Locate the network interface section and add a model line as shown:

```
<interface type='network'>
 ...
 <model type='e1000' />
</interface>
```

- Create the new virtual machine:

```
virsh define /tmp/new-guest.xml
virsh start new-guest
```

- Currently, KVM cannot disable virtualization extensions on a CPU while it is being taken down. Consequently, suspending a host running KVM-based virtual machines may cause the host to crash. (BZ#509809)
- The KSM module shipped in this release is a different version from the KSM module found on the latest upstream kernel versions. Newer features, such as exporting statistics on the /sys filesystem, that are implemented upstream are not in the version shipped in this release.
- The mute button in the audio control panel on a Windows virtual machine does not mute the sound. BZ#482570
- Hot-unplugging of PCI devices is not supported in this release. This feature will be introduced in a future update. (BZ#510679)
- When migrating KVM guests between hosts, the NX CPU feature setting on both source and destination must match. Migrating a guest between a host with the NX feature disabled (i.e. disabled in the BIOS settings) and a host with the NX feature enabled may cause the guest to crash. (BZ#516029)
- the application binary interface (ABI) between the KVM userspace (e.g. qemu-kvm) and the KVM kernel modules may change in future updates. Using the latest upstream qemu-kvm package is unsupported due to ABI differences. (BZ#515549)
- Devices using the qlge driver cannot be assigned to a KVM guest using KVM's PCI Device Driver assignment. (BZ#507689)

- the use of the qcow2 disk image format with KVM is considered a Technology Preview. (BZ#517880)
- Hotplugging emulated devices after migration may result in the virtual machine crashing after a reboot or the devices no longer being visible. (BZ#507191)
- Windows 2003 32-bit guests with more than 4GB of RAM may crash on reboot with the default qemu-kvm CPU settings. To work around this issue, configure a different CPU model on the management interface. (BZ#516762)
- The KVM modules from the **kmod-kvm** package do not support kernels prior to version 2.6.18-159.el5. Error messages similar to the following will be returned if attempting to install these modules on older kernels:

  ```
  FATAL: Error inserting kvm_intel
  (/lib/modules/2.6.18-155.el5/weak-updates/kmod-kvm/kvm-intel.ko): Unknown
  symbol in module, or unknown parameter (see dmesg)
  ```

  (BZ#509361)
- the kvm package has incorrect dependencies related to the **libgcrypt** package. Consequently, if the **libgcrypt** package installed on a system is earlier than version 1.4.4, the **qemu-kvm** process may refuse to start, returning a **libgcrypt initialization error** message. To work around this issue, update **libgcrypt** to the version provided by Red Hat Enterprise Linux 5.4. (BZ#503118)
- The KVM modules available in the **kmod-kvm** package are loaded automatically at boot time if the kmod-kvm package is installed. To make these KVM modules available after installing the **kmod-kvm** package the system either needs to be rebooted or the modules can be loaded manually by running the **/etc/sysconfig/modules/kvm.modules** script. (BZ#501543)
- Some Linux-based guests that use virtio virtual block devices may abort during installation, returning the error message: unhandled vm exit: 0x31 vcpu_id 0 To work around this issue, consider utilizing a different interface (other than virtio) for the guest virtual disk. (BZ#518081)
- RHEL5.x virtualization relies on etherboot for remote booting. Etherboot is an implementation of the pxe standard, but lacks some features that are present in the new gpxe boot technology which is not shipped with RHEL. It is possible to use the gpxe roms with RHEL 5.4. As an example, gpxe roms can be used to interpret requests generated by Microsoft RIS or WDS. All components present in RHEL5.4 are capable of booting gpxe roms. The roms can be obtained directly from http://rom-o-matic.net/, or other sources like the Fedora Project. BZ#509208
- The Preboot eXecution Environment (PXE) boot ROMs included with KVM are from the Etherboot project. Consequently, some bug fixes or features that are present on the newer gPXE project are not available on Etherboot. For example, Virtual Machines (VMs) cannot boot using Microsoft based PXE (ie. Remote Installation Services (RIS) or Windows Deployment Services (WDS)). (BZ#497692)
- The following QEMU / KVM features are currently disabled and not supported: (BZ#512837)
  - smb user directories
  - scsi emulation
  - "isapc" machine type
  - nested KVM guests
  - usb mass storage device emulation
  - usb wacom tablet emulation

- usb serial emulation
- usb network emulation
- usb bluetooth emulation
- device emulation for vmware drivers
- sb16, es1370, and ac97 sound card emulation
- bluetooth emulation

4.17. less

The less utility is a text file browser that resembles more, but with more capabilities ("less is more"). The less utility allows users to move backwards in the file as well as forwards. Because less need not read the entire input file before it starts, less starts up more quickly than text editors (vi, for example).

- The "less" command has been updated. Refer to Section 1.115, “ less ”. less no longer adds the "carriage return" character when wrapping long lines. Consequently, lines longer than the terminal width will be displayed incorrectly when browsing the file line per line. The command line option "--old-bot" forces less to behave as it did previously, with long text lines displayed correctly. (BZ#441691)

4.18. libvirt-cim

The libvirt-cim package is a Common Manageablity Programming Interface (CMPI) CIM provider that implements the Distributed Management Task Force's (DMTF's) System Virtualization, Partitioning and Clustering (SVPC) virtualization model. This package supports most of the features of libvirt and enables management of multiple platforms with a single provider.

- Selecting libvirt-cim package in the KVM group during installation will install the xen package as a dependency. To work around this issue do not select libvirt-cim during installation. After the installation is complete register the system to the Red Hat Network (RHN) and install the updated libvirt-cim package. (BZ#517579)

Note

libvirt-cim is an optional package in the KVM group and will not be installed if the group is selected. The package has to be selected manually from the optional packages list to be installed.

4.19. libvirt

Problem Description: 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.

- Volumes created using the libvirt storage API may not have an SELinux label that allows access by virtual machines. If an SELinux AVC denial is reported when starting a Xen or KVM guest, the adminstrator should either manually relabel the file/device, or add the file path(s) as rule to the SELinux policy using the 'semanage' tool. (BZ#510143)

4.20. lvm2

The lvm2 package contains support for Logical Volume Management (LVM).

The following are the Known Issues that apply to the lvm2 packages in Red Hat Enterprise Linux 5.4

- The **lvchange** command is used to change the attributes of a logical volume. Issuing the **lvchange** command on a volume group that contains a mirror or snapshot may result in messages similar to the following:

  ```
  Unable to change mirror log LV fail_secondary_mlog directly
  Unable to change mirror image LV fail_secondary_mimage_0 directly
  Unable to change mirror image LV fail_secondary_mimage_1 directly
  ```

  These messages can be safely ignored. (BZ#232499)

4.21. mesa

Mesa provides a 3D graphics API that is compatible with OpenGL. It also provides hardware-accelerated drivers for many popular graphics chips.

The following note applies to x86_64 Architectures:

- On an *IBM T61* laptop, Red Hat recommends that you refrain from clicking the **glxgears** window (when **glxgears** is run). Doing so can lock the system.

  To prevent this from occurring, disable the tiling feature. To do so, add the following line in the **Device** section of **/etc/X11/xorg.conf**:

  ```
  Option "Tiling" "0"
  ```

  (BZ#444508)

4.22. mkinitrd

The mkinitrd utility creates file system images for use as initial ramdisk (initrd) images.

- When using an encrypted device, the following error message may be reported during bootup:

  ```
  insmod: error inserting '/lib/aes_generic.ko': -1 File exists
  ```

  This message can safely be ignored. (BZ#466296)

- Installation using a Multiple Device (MD) RAID on top of multipath will result in a machine that cannot boot. Multipath to Storage Area Network (SAN) devices which provide RAID internally are not affected. (BZ#467469)

The following note applies to s390x Architectures:

- When installing Red Hat Enterprise Linux 5.4, the following errors may be returned in **install.log**:

  ```
  Installing kernel-2.6.18-158.el5.s390x
  cp: cannot stat `/sbin/dmraid.static': No such file or directory
  ```

  This message can be safely ignored.

4.23. openib

The OpenFabrics Alliance Enterprise Distribution (OFED) is a collection of Infiniband and iWARP hardware diagnostic utilities, the Infiniband fabric management daemon, Infiniband/iWARP kernel module loader, and libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology. Red Hat Enterprise Linux uses the OFED software stack as its complete stack for Infiniband/iWARP/RDMA hardware support.

The following note applies to the ia64 Architectures:

- Running **perftest** will fail if different CPU speeds are detected. As such, you should disable CPU speed scaling before running **perftest**. (BZ#433659)

4.24. openmpi

Open MPI, MVAPICH, and MVAPICH2 are all competing implementations of the Message Passing Interface (MPI) standard. MVAPICH implements version 1 of the MPI standard, while Open MPI and MVAPICH2 both implement the later, version 2 of the MPI standard.

- **mvapich** and **mvapich2** in Red Hat Enterprise Linux 5 are compiled to support only *InfiniBand/iWARP* interconnects. Consequently, they will not run over ethernet or other network interconnects. (BZ#466390)
- When upgrading openmpi using yum, the following warning may be returned:

  ```
  cannot open `/tmp/openmpi-upgrade-version.*' for reading: No such file or
  directory
  ```

  The message is harmless and can be safely ignored. (BZ#463919)
- A bug in previous versions of **openmpi** and **lam** may prevent you from upgrading these packages. This bug manifests in the following error (when attempting to upgrade **openmpi** or **lam**:

  ```
  error: %preun(openmpi-[version]) scriptlet failed, exit status 2
  ```

  As such, you need to manually remove older versions of **openmpi** and **lam** in order to install their latest versions. To do so, use the following **rpm** command:

  rpm -qa | grep '^openmpi-\|^lam-' | xargs rpm -e --noscripts --allmatches
  (BZ#433841)

4.25. pdksh

The Public Domain Korn SHell implements the ksh-88 programming language for both interactive and shell script use.

- pdksh — a new package in Red Hat Enterprise Linux 5.4 — does not recognize the keyword **source** in scripts. However, the **/etc/profile.d/kde.sh** script uses the **source** keyword in the line **source /etc/sysconfig/prelink**. Consequently, if a user is using pdksh as their shell, and KDE is installed, the following error message will be returned in login shells:

  ```
  ksh: /etc/profile.d/kde.sh[7]: source: not found
  ```

  To work around this issue, change the

```
source /etc/sysconfig/prelink
```

line in the **/etc/profile.d/kde.sh** script to

```
. /etc/sysconfig/prelink
```

The keyword **.** is an alias for **source** in all Bourne compatible shells including **bash**, **AT&T ksh**, and **pdksh**.

This issue will be resolved in an upcoming update to Red Hat Enterprise Linux 5.4. (BZ#510374)

4.26. qspice

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built 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 and from a wide variety of machine architectures.

- Occasionally, the video compression algorithm used by SPICE starts when the guest is accessing text instead of video or moving content. This causes the text to appear blurry or difficult to read. (BZ#493375)

4.27. rsyslog

rsyslog is an enhanced multi-threaded system logging utility (syslogd) which supports MySQL, syslog/tcp, RFC 3195, permitted sender lists, filtering on any message part, and fine-grain output format control. It is quite compatible to stock sysklogd, and can be used as a drop-in replacement. Its advanced features make it suitable for enterprise-class, encryption-protected syslog relay chains while at the same time being very easy for the novice user to set up.

- Currently, rsyslog is unable to handle a large number of clients; SGI's ICE clusters are known to cause overload resulting in messages being lost. (BZ#475217)

4.28. sblim

SBLIM stands for Standards-Based Linux Instrumentation for Manageability. It consists of a set of standards-based, Web-Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via a CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.

- when the **sblim-cmpi-dhcp** package is installed, it modifies the files under **/var/lib/Pegasus** owned by the **tog-pegasus** package. Previously, when **sblim** was installed in the course of an "everything" installation of Red Hat Enterprise Linux 5 on the PowerPC architecture, the modifications that **sblim** made in the **/var/lib/Pegasus** directory prevented the post-install scriptlet from completing the provider-register commands. In turn, this would prevent installation of Red Hat Enterprise Linux 5 from completing. The provider-register commands are no longer provided in the post-install scriptlet, therefore avoiding this situation and allowing installation of the operating system to complete normally. Users of SBLIM who need to register provider modules for tog-pegasus should register these modules manually by running the following command as root:

```
/usr/share/sblim-cmpi-dhcp/provider-register.sh -t pegasus -v -n
"root/PG_InterOp" -r
```

```
/usr/share/sblim-cmpi-dhcp/Linux_DHCPRegisteredProfile.registration
/usr/share/sblim-cmpi-dhcp/Linux_DHCPElementConformsToProfile.registration
-m
/usr/share/sblim-cmpi-dhcp/Linux_DHCPService.mof
/usr/share/sblim-cmpi-dhcp/Linux_DHCPRegisteredProfile.mof
/usr/share/sblim-cmpi-dhcp/Linux_DHCPElementConformsToProfile.mof
```

Accordingly, deregister modules before update/remove of the sblim-cmpi-dhcp package with following command as root:

```
/usr/share/sblim-cmpi-dhcp/provider-register.sh -d -t pegasus -n
"root/PG_InterOp" -r
/usr/share/sblim-cmpi-dhcp/Linux_DHCPRegisteredProfile.registration
/usr/share/sblim-cmpi-dhcp/Linux_DHCPElementConformsToProfile.registration
-m
/usr/share/sblim-cmpi-dhcp/Linux_DHCPService.mof
/usr/share/sblim-cmpi-dhcp/Linux_DHCPRegisteredProfile.mof
/usr/share/sblim-cmpi-dhcp/Linux_DHCPElementConformsToProfile.mof
```

4.29. selinux-policy

The selinux-policy packages contain the rules that govern how confined processes run on the system.

- When upgrading from Red Hat Enterprise Linux 4 Workstation to 5 Server, **OpenOffice** will no longer work correctly with SELinux. This is because the Red Hat Enterprise Linux version of **OpenOffice** is built using an incorrect library. As a result, SELinux will prevent **OpenOffice** from accessing any shared libraries, causing **OpenOffice** to fail.

  To work around this, update the SELinux context to allow **OpenOffice** to access shared libraries. To do so, run the following commands:

  `semanage fcontext -a -t textrel_shlib_t '/usr/lib/ooo-1.1(/.*)?'`

  `semanage fcontext -a -t textrel_shlib_t '/usr/lib64/ooo-1.1(/.*)?'`

  `restorecon -Rv /usr/lib/ooo-1.19`

  `restorecon -Rv /usr/lib64/ooo-1.19`

  Alternatively, you can also upgrade your **OpenOffice** to a correct version compatible with SELinux in Red Hat Enterprise Linux 5. You can do this by subscribing to the "Productivity App" child channel in Red Hat Network and running the following command:

  `yum install openoffice-{base,calc,draw,emailmerge,graphicfilter,headless,impress,javafilter,math,pyuno,writer,xsltfilter}`

  (BZ#477103)

4.30. systemtap

SystemTap provides an instrumentation infrastructure for systems running the Linux 2.6 kernel. It allows users to write scripts that probe and trace system events for monitoring and profiling purposes. SystemTap's framework allows users to investigate and monitor a wide variety of wide variety of kernel functions, system calls, and other evens that occur in both kernel-space and user-space.

The following are the Known Issues that apply to the systemtap package in Red Hat Enterprise Linux 5.4

- Running some user-space probe test cases provided by the **systemtap-testsuite** package fail with an **Unknown symbol in module** error on some architectures. These test cases include (but are not limited to):

  - **systemtap.base/uprobes.exp**
  - **systemtap.base/bz10078.exp**
  - **systemtap.base/bz6850.exp**
  - **systemtap.base/bz5274.exp**

  Because of a known bug in the latest SystemTap update, new SystemTap installations do not unload old versions of the **uprobes.ko** module. Some updated user-space probe tests provided by the systemtap-testsuite package use symbols available only in the latest **uprobes.ko** module (also provided by the latest SystemTap update). As such, running these user-space probe tests result in the error mentioned earlier.

  If you encounter this error, simply run **rmmod uprobes** to manually remove the older **uprobes.ko** module before running the user-space probe test again.(BZ#499677)

- SystemTap currently uses GCC to probe user-space events. GCC is, however, unable to provide debuggers with precise location list information for parameters. In some cases, GCC also fails to provide visibility on some parameters. As a consequence, SystemTap scripts that probe user-space may return inaccurate readings. (BZ#239065)

4.31. udev

udev provides a user-space API and implements a dynamic device directory, providing only the devices present on the system. udev replaces devfs in order to provide greater hot plug functionality. Netlink is a datagram oriented service, used to transfer information between kernel modules and user-space processes.

- A bug in the updated **/etc/udev/rules.d/50-udev.rules** file prevents the creation of persistent names for tape devices with numbers higher than 9 in their names. For example, a persistent name will not be created for a tape device with a name of **nst12**.

  To work around this, add an asterisk (*) after each occurrence of the string **nst[0-9]** in **/etc/udev/rules.d/50-udev.rules**. (BZ#231990)

4.32. virt-manager

- Fully virtualized guests created through **virt-manager** may sometimes prevent the mouse from moving freely throughout the screen. To work around this, use **virt-manager** to configure a USB tablet device for the guest. (BZ#223805)

4.33. virtio-win

VirtIO para-virtualized Windows(R) drivers for 32-bit and 64-bit Windows (R) guests.

- Low performance with UDP messages larger than 1024 is a known Microsoft issue: http://support.microsoft.com/default.aspx/kb/235257. For the message larger than 1024 bytes follow the workaround procedure detailed in the above Microsoft knowledgebase article.

(BZ#496592)

- Installation of Windows XP with the floppy containing guest drivers (in order to get the virtio-net drivers installed as part of the installation), will return messages stating that the viostor.sys file could not be found. viostor.sys is not part of the network drivers, but is on the same floppy as portions of the virtio-blk drivers. These messages can be safely ignored, simply accept the installation's offer to reboot, and the installation will continue normally. BZ#513160

4.34. xen

- As of Red Hat Enterprise Linux 5.4, PCI devices connected to a single PCI-PCI bridge can no longer be assigned to different PV guests. If the old, unsafe behaviour is required, disable pci-dev-assign-strict-check in /etc/xen/xend-config.sxp. (BZ#508310)
- Save operations should not be attempted on paused Xen domains. This will cause Xend to hang. (BZ#504910)
- In live migrations of paravirtualized guests, time-dependent guest processes may function improperly if the corresponding hosts' (dom0) times are not synchronized. Use NTP to synchronize system times for all corresponding hosts before migration. (BZ#426861)
- The Red Hat Enterprise Linux 3 kernel does not include SWIOTLB support. SWIOTLB support is required for Red Hat Enterprise Linux 3 guests to support more than 4GB of memory on AMD Opteron and Athlon-64 processors. Consequently, Red Hat Enterprise Linux 3 guests are limited to 4GB of memory on AMD processors. (BZ#504187)
- When setting up interface bonding on **dom0**, the default **network-bridge** script may cause bonded network interfaces to alternately switch between **unavailable** and **available**. This occurrence is commonly known as *flapping*.

  To prevent this, replace the standard **network-script** line in **/etc/xen/xend-config.sxp** with the following line:

  ```
  (network-script network-bridge-bonding netdev=bond0)
  ```

  Doing so will disable the *netloop* device, which prevents Address Resolution Protocol (ARP) monitoring from failing during the address transfer process. (BZ#429154)(BZ#429154)
- The Hypervisor outputs messages regarding attempts by any guest to write to an MSR. Such messages contain the statement **Domain attempted WRMSR**. These messages can be safely ignored; furthermore, they are rate limited and should pose no performance risk. (BZ#477647)
- Red Hat advises that you avoid removing a block device from a guest while the device is in use. Doing so causes Xend to lose domain information for the guest. (BZ#476164)

The following note applies to x86_64 Architectures:

- Installing Red Hat Enterprise Linux 3.9 on a fully virtualized guest may be extremely slow. In addition, booting up the guest after installation may result in **hda: lost interrupt** errors.

  To avoid this bootup error, configure the guest to use the SMP kernel. (BZ#249521)

4.35. xorg-x11-drv-i810

xorg-x11-drv-i810 is an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

- Running a screensaver or resuming a suspended laptop with an external monitor attached may result in a blank screen or a brief flash followed by a blank screen. If this occurs with the screensaver, the prompt for your password is being obscured, the password can still be entered blindly to get back to the desktop. To work around this issue, physically disconnect the external monitor and then press the video hotkey (usually Fn-F7) to rescan the available outputs, before suspending the laptop.

The following notes apply to x86_64 Architectures:

- If your system uses an *Intel 945GM* graphics card, do not use the **`i810`** driver. You should use the default **`intel`** driver instead. (BZ#468218)

- On dual-GPU laptops, if one of the graphics chips is Intel-based, the Intel graphics mode cannot drive any external digital connections (including HDMI, DVI, and DisplayPort). This is a hardware limitation of the Intel GPU. If you require external digital connections, configure the system to use the discrete graphics chip (in the BIOS). (BZ#468259)

4.36. xorg-x11-drv-nv

xorg-x11-drv-nv provides a driver for NVIDIA cards for the X.org implementation of the X Window System.

- Improvements have been made to the 'nv' driver, enhancing suspend and resume support on some systems equipped with nVidia GeForce 8000 and 9000 series devices. Due to technical limitations, this will not enable suspend/resume on all hardware. (BZ#414971)

The following note applies to x86_64 Architectures:

- Some machines that use *NVIDIA* graphics cards may display corrupted graphics or fonts when using the graphical installer or during a graphical login. To work around this, switch to a virtual console and back to the original X host. (BZ#222737, BZ#221789)

4.37. xorg-x11-drv-vesa

xorg-x11-drv-vesa is a video driver for the X.Org implementation of the X Window System. It is used as a fallback driver for cards with no native driver, or when the native driver does not work.

The following note applies to x86 Architectures:

- When running the bare-metal (non-Virtualized) kernel, the X server may not be able to retrieve **`EDID`** information from the monitor. When this occurs, the graphics driver will be unable to display resolutions highers than 800x600.

  To work around this, add the following line to the **`ServerLayout`** section of **`/etc/X11/xorg.conf`**:

  ```
  Option "Int10Backend" "x86emu"
  ```

  (BZ#236416)

Appendix A. Package Manifest

This appendix is a list of all package changes since the release of Red Hat Enterprise Linux 5.3

A.1. Added Packages

blktrace-1.0.0-6.el5

- Group: *Development/System*
- Summary: *Utilities for performing block layer IO tracing in the linux kernel*
- Description: *blktrace is a block layer IO tracing mechanism which provides detailed information about request queue operations to user space. This package includes both blktrace, a utility which gathers event traces from the kernel; and blkparse, a utility which formats trace data collected by blktrace. You should install the blktrace package if you need to gather detailed information about IO patterns.*

celt051-0.5.1.3-0.el5

- Group: *System Environment/Libraries*
- Summary: *An audio codec for use in low-delay speech and audio communication*
- Description: *CELT (Constrained Energy Lapped Transform) is an ultra-low delay audio codec designed for realtime transmission of high quality speech and audio. This is meant to close the gap between traditional speech codecs (such as Speex) and traditional audio codecs (such as Vorbis).*

etherboot-5.4.4-10.el5

- Group: *Development/Tools*
- Summary: *Etherboot collection of boot roms*
- Description: *Etherboot is a software package for creating ROM images that can download code over an Ethernet network to be executed on an x86 computer. Many network adapters have a socket where a ROM chip can be installed. Etherboot is code that can be put in such a ROM*

fcoe-utils-1.0.7-4.el5

- Group: *Applications/System*
- Summary: *Fibre Channel over Ethernet utilities*
- Description: *Fibre Channel over Ethernet utilities fcoeadm - command line tool for configuring FCoE interfaces fcoemon - service to configure DCB Ethernet QOS filters, works with dcbd*

fuse-2.7.4-8.el5

- Group: *System Environment/Base*
- Summary: *File System in Userspace (FUSE) utilities*
- Description: *With FUSE it is possible to implement a fully functional filesystem in a userspace program. This package contains the FUSE userspace tools to mount a FUSE filesystem.*

gcc44-4.4.0-6.el5

- Group: *Development/Languages*
- Summary: *Preview of GCC version 4.4*
- Description: *The gcc44 package contains preview of the GNU Compiler Collection version 4.4.*

gnupg2-2.0.10-3.el5

- Group: *Applications/System*
- Summary: *Utility for secure communication and data storage*
- Description: *GnuPG is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures. It includes an advanced key management facility and is compliant with the proposed OpenPGP Internet standard as described in RFC2440 and the S/MIME standard as described by several RFCs. GnuPG 2.0 is the stable version of GnuPG integrating support for OpenPGP and S/MIME. It does not conflict with an installed 1.x OpenPGP-only version. GnuPG 2.0 is a newer version of GnuPG with additional support for S/MIME. It has a different design philosophy that splits functionality up into several modules. Both versions may be installed simultaneously without any conflict (gpg is called gpg2 in GnuPG 2). In fact, the gpg version from GnuPG 1.x is able to make use of the gpg-agent as included in GnuPG 2 and allows for seamless passphrase caching. The advantage of GnupG 1.x is its smaller size and no dependency on other modules at run and build time.*

hmaccalc-0.9.6-1.el5

- Group: *System Environment/Base*
- Summary: *Tools for computing and checking HMAC values for files*
- Description: *The hmaccalc package contains tools which can calculate HMAC (hash-based message authentication code) values for files. The names and interfaces are meant to mimic the sha*sum tools provided by the coreutils package.*

iasl-20061109-5.el5

- Group: *Development/Languages*
- Summary: *Intel ASL compiler/decompiler*
- Description: *iasl compiles ASL (ACPI Source Language) into AML (ACPI Machine Language), which is suitable for inclusion as a DSDT in system firmware. It also can disassemble AML, for debugging purposes.*

kvm-83-105.el5

- Group: *Development/Tools*
- Summary: *Kernel-based Virtual Machine*
- Description: *KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.*

libassuan-1.0.4-5.el5

- Group: *System Environment/Libraries*
- Summary: *GnuPG IPC library*

- Description: *This is the IPC library used by GnuPG 2, GPGME and a few other packages.*

libhbaapi-2.2-4.el5

- Group: *System Environment/Libraries*
- Summary: *SNIA HBAAPI library*
- Description: *The SNIA HBA API library. C-level project to manage Fibre Channel Host Bus Adapters.*

libhbalinux-1.0.7-3.el5

- Group: *System Environment/Libraries*
- Summary: *FC-HBAAPI implementation using scsi_transport_fc interfaces*
- Description: *SNIA HBAAPI vendor library built on top of the scsi_transport_fc interfaces*

libksba-1.0.5-2.el5

- Group: *System Environment/Libraries*
- Summary: *X.509 library*
- Description: *KSBA is a library designed to build software based on the X.509 and CMS protocols.*

libpciaccess-0.10.5-2.el5

- Group: *System Environment/Libraries*
- Summary: *PCI access library*
- Description: *libpciaccess is a library for portable PCI access routines across multiple operating systems.*

log4cpp-1.0-4.el5

- Group: *Development/Libraries*
- Summary: *C++ logging library*
- Description: *A library of C++ classes for flexible logging to files, syslog, IDSA and other destinations. It is modeled after the Log for Java library (http://www.log4j.org), staying as close to their API as is reasonable.*

pdksh-5.2.14-36.el5

- Group: *System Environment/Shells*
- Summary: *A public domain shell implementing ksh-88*
- Description: *The pdksh package contains public domain implementation of ksh-88. The ksh shell is a command interpreter intended for both interactive and shell script use. Ksh's command language is a superset of the sh shell language. Pdksh is unmaintained since 1998 and is obsoleted by ksh package.*

perl-Sys-Virt-0.2.0-4.el5

- Group: *Development/Libraries*

- Summary: *Perl bindings for the libvirt library*
- Description: *The Sys::Virt module provides a Perl XS binding to the libvirt virtual machine management APIs. This allows machines running within arbitrary virtualization containers to be managed with a consistent API.*

pinentry-0.7.3-3.el5

- Group: *Applications/System*
- Summary: *Collection of simple PIN or passphrase entry dialogs*
- Description: *Pinentry is a collection of simple PIN or passphrase entry dialogs which utilize the Assuan protocol as described by the aegypten project; see http://www.gnupg.org/aegypten/ for details. This package contains the curses (text) based version of the PIN entry dialog.*

pth-2.0.7-6.el5

- Group: *System Environment/Libraries*
- Summary: *The GNU Portable Threads library*
- Description: *Pth is a very portable POSIX/ANSI-C based library for Unix platforms which provides non-preemptive priority-based scheduling for multiple threads of execution ("multithreading") inside server applications. All threads run in the same address space of the server application, but each thread has it's own individual program-counter, run-time stack, signal mask and errno variable.*

qcairo-1.8.7.1-3.el5

- Group: *System Environment/Libraries*
- Summary: *A 2D graphics library*
- Description: *This is a version of the cairo 2D graphics library, with additional features required to support the implementation of the spice protocol. Cairo is a 2D graphics library designed to provide high-quality display and print output. Currently supported output targets include the X Window System, OpenGL (via glitz), in-memory image buffers, and image files (PDF, PostScript, and SVG). Cairo is designed to produce consistent output on all output media while taking advantage of display hardware acceleration when available (e.g. through the X Render Extension or OpenGL).*

qffmpeg-0.4.9-0.15.20080908.el5

- Group: *Applications/Multimedia*
- Summary: *Stripped-down fork of ffmpeg for libspice*
- Description: *This is a stripped down version of upstream FFMPEG including only the codecs used by SPICE in order to avoid inadvertantly bundling or shipping any encumbered code or binaries.*

qpixman-0.13.3-4.el5

- Group: *System Environment/Libraries*
- Summary: *Modified version of pixman for spice*
- Description: *Qpixman is a pixel manipulation library for X and cairo.*

qspice-0.3.0-39.el5

- Group: *User Interface/Desktops*
- Summary: *An implementation of the Simple Protocol for Independent Computing Environments*
- Description: *The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments 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.*

rds-tools-1.4-2.el5

- Group: *Applications/System*
- Summary: *RDS support tools*
- Description: *Various tools for support of the RDS (Reliable Datagram Socket) API. RDS is specific to InfiniBand and iWARP networks and does not work on non-RDMA hardware.*

xorg-x11-drv-qxl-0.0.4-1.1.el5

- Group: *User Interface/X Hardware Support*
- Summary: *Xorg X11 qxl video driver*
- Description: *X.Org X11 qxl video driver.*

xorg-x11-xdm-1.0.5-6.el5

- Group: *User Interface/X*
- Summary: *X.Org X11 xdm - X Display Manager*
- Description: *X.Org X11 xdm - X Display Manager*

A.2. Dropped Packages

gcc43-4.3.2-7.el5

- Group: *Development/Languages*
- Summary: *Preview of GCC version 4.3*
- Description: *The gcc43 package contains preview the GNU Compiler Collection version 4.3.*

A.3. Updated Packages

NetworkManager-0.7.0-3.el5 - NetworkManager-0.7.0-9.el5

- Group: *System Environment/Base*
- Summary: *Network connection manager and user applications*
- Description: *NetworkManager attempts to keep an active network connection available at all times. It is intended only for the desktop use-case, and is not intended for usage on servers. The point of NetworkManager is to make networking configuration and setup as painless and automatic as possible. If using DHCP, NetworkManager is intended to replace default routes, obtain IP addresses from a DHCP server, and change nameservers whenever it sees fit.*
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

OpenIPMI-2.0.6-11.el5 - OpenIPMI-2.0.16-5.el5

- Group: *System Environment/Base*
- Summary: *OpenIPMI (Intelligent Platform Management Interface) library and tools*
- Description: *The Open IPMI project aims to develop an open code base to allow access to platform information using Intelligent Platform Management Interface (IPMI). This package contains the tools of the OpenIPMI project.*
- Added Dependencies:
  - desktop-file-utils
  - tcl-devel
  - tkinter
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

acpid-1.0.4-7.el5 - acpid-1.0.4-9.el5

- Group: *System Environment/Daemons*
- Summary: *ACPI Event Daemon*
- Description: *acpid is a daemon that dispatches ACPI events to user-space programs.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

aide-0.13.1-2.0.4.el5 - aide-0.13.1-4.el5

- Group: *Applications/System*
- Summary: *Intrusion detection environment*
- Description: *AIDE (Advanced Intrusion Detection Environment) is a file integrity checker and intrusion detection program.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

amanda-2.5.0p2-4 - amanda-2.5.0p2-8.el5

- Group: *Applications/System*
- Summary: *A network-capable tape backup solution.*
- Description: *AMANDA, the Advanced Maryland Automatic Network Disk Archiver, is a backup system that allows the administrator of a LAN to set up a single master backup server to back up multiple hosts to one or more tape drives or disk files. AMANDA uses native dump and/or GNU tar facilities and can back up a large number of workstations running multiple versions of Unix. Newer versions of AMANDA (including this version) can use SAMBA to back up Microsoft(TM) Windows95/NT hosts. The amanda package contains the core AMANDA programs and will need to be installed on both AMANDA clients and AMANDA servers. Note that you will have to install the amanda-client and/or amanda-server packages as well.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

anaconda-11.1.2.168-1 - anaconda-11.1.2.195-1

- Group: *Applications/System*
- Summary: *Graphical system installer*
- Description: *The anaconda package contains the program which was used to install your system. These files are of little use on an already installed system.*
- Added Dependencies:
  - iscsi-initiator-utils >= 6.2.0.871-0.0
  - libdhcp-devel >= 1.20-10
  - libdhcp6client >= 1.0.10-17
- Removed Dependencies:
  - iscsi-initiator-utils >= 6.2.0.868-0.9
  - libdhcp-devel >= 1.20-5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

apr-1.2.7-11 - apr-1.2.7-11.el5_3.1

- Group: *System Environment/Libraries*
- Summary: *Apache Portable Runtime library*
- Description: *The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines, forming a system portability layer to as many operating systems as possible, including Unices, MS Win32, BeOS and OS/2.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

apr-util-1.2.7-7.el5 - apr-util-1.2.7-7.el5_3.2

- Group: *System Environment/Libraries*
- Summary: *Apache Portable Runtime Utility library*
- Description: *The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines. This library contains additional utility interfaces for APR; including support for XML, LDAP, database interfaces, URI parsing and more.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aspell-nl-0.1e-1.fc6 - aspell-nl-0.1e-2.el5

- Group: *Applications/Text*
- Summary: *Dutch dictionaries for Aspell*
- Description: *Provides the word list/dictionaries for the following: Dutch*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

audit-1.7.7-6.el5 - audit-1.7.13-2.el5

- Group: *System Environment/Daemons*
- Summary: *User space tools for 2.6 kernel auditing*
- Description: *The audit package contains the user space utilities for storing and searching the audit records generate by the audit subsystem in the Linux 2.6 kernel.*
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

authconfig-5.3.21-5.el5 - authconfig-5.3.21-6.el5

- Group: *System Environment/Base*
- Summary: *Command line tool for setting up authentication from network services*
- Description: *Authconfig is a command line utility which can configure a workstation to use shadow (more secure) passwords. Authconfig can also configure a system to be a client for certain networked user information and authentication schemes.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

authd-1.4.3-9 - authd-1.4.3-14

- Group: *System Environment/Daemons*
- Summary: *a RFC 1413 ident protocol daemon*
- Description: *authd is a small and fast RFC 1413 ident protocol daemon with both xinetd server and interactive modes that supports IPv6 and IPv4 as well as the more popular features of pidentd.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

autofs-5.0.1-0.rc2.102 - autofs-5.0.1-0.rc2.131.el5

- Group: *System Environment/Daemons*
- Summary: *A tool for automatically mounting and unmounting filesystems.*
- Description: *autofs is a daemon which automatically mounts filesystems when you use them, and unmounts them later when you are not using them. This can include network filesystems, CD-ROMs, floppies, and so forth.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

avahi-0.6.16-1.el5 - avahi-0.6.16-6.el5

- Group: *System Environment/Base*
- Summary: *Local network service discovery*
- Description: *Avahi is a system which facilitates service discovery on a local network -- this means that you can plug your laptop or computer into a network and instantly be able to view other people who you can chat with, find printers to print to or find files being shared. This kind of technology is already found in MacOS X (branded 'Rendezvous', 'Bonjour' and sometimes 'ZeroConf') and is very convenient.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind-9.3.4-10.P1.el5 - bind-9.3.6-4.P1.el5

- Group: *System Environment/Daemons*
- Summary: *The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server.*

- Description: *BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.*
- No added dependencies
- Removed Dependencies:
  - glibc-kernheaders >= 2.4-7.10
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

binutils-2.17.50.0.6-9.el5 - binutils-2.17.50.0.6-12.el5

- Group: *Development/Tools*
- Summary: *A GNU collection of binary utilities.*
- Description: *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), 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).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

busybox-1.2.0-4.el5 - busybox-1.2.0-7.el5

- Group: *System Environment/Shells*
- Summary: *Statically linked binary providing simplified versions of system commands*
- Description: *Busybox is a single binary which includes versions of a large number of system commands, including a shell. This package can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.*

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cman-2.0.98-1.el5 - cman-2.0.115-1.el5

- Group: *System Environment/Base*
- Summary: *cman - The Cluster Manager*
- Description: *cman - The Cluster Manager*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cmirror-1.1.36-1.el5 - cmirror-1.1.39-2.el5

- Group: *System Environment/Base*
- Summary: *cmirror - The Cluster Mirror Package*
- Description: *cmirror - Cluster Mirroring*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cmirror-kmod-0.1.21-10.el5 - cmirror-kmod-0.1.22-1.el5

- Group: *System Environment/Kernel*
- Summary: *cmirror kernel modules*
- Description: *cmirror-kmod - The Cluster Mirror kernel modules*
- Added Dependencies:
  - kernel-devel-ia64 = 2.6.18-159.el5
  - kernel-xen-devel-ia64 = 2.6.18-159.el5
- Removed Dependencies:
  - kernel-devel-ia64 = 2.6.18-128.el5
  - kernel-xen-devel-ia64 = 2.6.18-128.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

conga-0.12.1-7.el5 - conga-0.12.2-6.el5

- Group: *System Environment/Base*
- Summary: *Remote Management System*
- Description: *Conga is a project developing management system for remote stations. It consists of luci, https frontend, and ricci, secure daemon that dispatches incoming messages to underlying management modules.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

coreutils-5.97-19.el5 - coreutils-5.97-23.el5

- Group: *System Environment/Base*
- Summary: *The GNU core utilities: a set of tools commonly used in shell scripts*

- Description: *These are the GNU core utilities. This package is the combination of the old GNU fileutils, sh-utils, and textutils packages.*
- Added Dependencies:
  - libattr-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cpio-2.6-20 - cpio-2.6-23.el5

- Group: *Applications/Archiving*
- Summary: *A GNU archiving program.*
- Description: *GNU cpio copies files into or out of a cpio or tar archive. Archives are files which contain a collection of other files plus information about them, such as their file name, owner, timestamps, and access permissions. The archive can be another file on the disk, a magnetic tape, or a pipe. GNU cpio supports the following archive formats: binary, old ASCII, new ASCII, crc, HPUX binary, HPUX old ASCII, old tar and POSIX.1 tar. By default, cpio creates binary format archives, so that they are compatible with older cpio programs. When it is extracting files from archives, cpio automatically recognizes which kind of archive it is reading and can read archives created on machines with a different byte-order. Install cpio if you need a program to manage file archives.*
- Added Dependencies:
  - rmt
  - rsh
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cpuspeed-1.2.1-5.el5 - cpuspeed-1.2.1-8.el5

- Group: *System Environment/Base*
- Summary: *CPU frequency adjusting daemon*

- Description: *cpuspeed is a daemon that dynamically changes the speed of your processor(s) depending upon its current workload if it is capable (needs Intel Speedstep, AMD PowerNow!, or similar support). This package also supports enabling cpu frequency scaling via in-kernel governors on Intel Centrino and AMD Athlon64/Opteron platforms.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

crash-4.0-7.2.3 - crash-4.0-8.9.1.el5

- Group: *Development/Debuggers*
- Summary: *crash utility for live systems; netdump, diskdump, kdump, LKCD or mcore dumpfiles*
- Description: *The core analysis suite is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cryptsetup-luks-1.0.3-4.el5 - cryptsetup-luks-1.0.3-5.el5

- Group: *Applications/System*
- Summary: *A utility for setting up encrypted filesystems*
- Description: *This package contains cryptsetup, a utility for setting up encrypted filesystems using Device Mapper and the dm-crypt target.*
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cscope-15.5-15.fc6.1 - cscope-15.5-15.1.el5_3.1

- Group: *Development/Tools*
- Summary: *C source code tree search and browse tool*
- Description: *cscope is a mature, ncurses based, C source code tree browsing tool. It allows users to search large source code bases for variables, functions, macros, etc, as well as perform general regex and plain text searches. Results are returned in lists, from which the user can select individual matches for use in file editing.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cups-1.3.7-8.el5 - cups-1.3.7-11.el5

- Group: *System Environment/Daemons*
- Summary: *Common Unix Printing System*
- Description: *The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

curl-7.15.5-2.el5 - curl-7.15.5-2.1.el5_3.5

- Group: *Applications/Internet*
- Summary: *A utility for getting files from remote servers (FTP, HTTP, and others).*
- Description: *cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict 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.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cvs-1.11.22-5.el5 - cvs-1.11.22-7.el5

- Group: *Development/Tools*
- Summary: *A version control system.*
- Description: *CVS (Concurrent Versions System) is a version control system that can record the history of your files (usually, but not always, source code). CVS only stores the differences between versions, instead of every version of every file you have ever created. CVS also keeps a log of who, when, and why changes occurred. CVS is very helpful for managing releases and controlling the concurrent editing of source files among multiple authors. Instead of providing version control for a collection of files in a single directory, CVS provides version control for a hierarchical collection of directories consisting of revision controlled files. These directories and files can then be combined together to form a software release.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cyrus-imapd-2.3.7-2.el5 - cyrus-imapd-2.3.7-7.el5

- Group: *System Environment/Daemons*
- Summary: *A high-performance mail server with IMAP, POP3, NNTP and SIEVE support*
- Description: *The cyrus-imapd package contains the core of the Cyrus IMAP server. It is a scaleable enterprise mail system designed for use from small to large enterprise environments using standards-based internet mail technologies. A full Cyrus IMAP implementation allows a seamless mail and bulletin board environment to be set up across multiple servers. It differs from other IMAP server implementations in that it is run on "sealed" servers, where users are not normally permitted to log in and have no system account on the server. The mailbox database is stored in parts of the filesystem that are private to the Cyrus IMAP server. All user access to mail is through software using the IMAP, POP3 or KPOP protocols. It also includes support for virtual domains, NNTP, mailbox annotations, and much more. The private mailbox database design gives the server large advantages in efficiency, scalability and administratability. Multiple concurrent read/write connections to the same mailbox are permitted. The server supports access control lists on mailboxes and storage quotas on mailbox hierarchies. The Cyrus IMAP server supports the IMAP4rev1 protocol described in RFC 3501. IMAP4rev1 has been approved as a proposed standard. It supports any authentication mechanism available from the SASL library, imaps/pop3s/nntps (IMAP/POP3/NNTP encrypted using SSL and TLSv1) can be used for security. The server supports single instance store where possible when an email message is addressed to multiple recipients, SIEVE provides server side email filtering.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cyrus-sasl-2.1.22-4 - cyrus-sasl-2.1.22-5.el5

- Group: *System Environment/Libraries*
- Summary: *The Cyrus SASL library.*
- Description: *The cyrus-sasl package contains the Cyrus implementation of SASL. SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

dapl-2.0.13-4.el5 - dapl-2.0.19-2.el5

- Group: *System Environment/Libraries*
- Summary: *Library providing access to the DAT 1.2 and 2.0 APIs*
- Description: *libdat and libdapl provide a userspace implementation of the DAT 1.2 and 2.0 API that is built to natively support InfiniBand/iWARP network technology.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4
  - librdmacm-devel >= 1.0.8-5
- Removed Dependencies:
  - libibverbs-devel >= 1.1
  - librdmacm-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

db4-4.3.29-9.fc6 - db4-4.3.29-10.el5

- Group: *System Environment/Libraries*
- Summary: *The Berkeley DB database library (version 4) for C.*
- Description: *The Berkeley Database (Berkeley DB) is a programmatic toolkit that provides embedded database support for both traditional and client/server applications. The Berkeley DB includes B+tree, Extended Linear Hashing, Fixed and Variable-length record access methods, transactions, locking, logging, shared memory caching, and database recovery. The Berkeley DB supports C, C++, Java, and Perl APIs. It is used by many applications, including Python and Perl, so this should be installed on all systems.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

device-mapper-1.02.28-2.el5 - device-mapper-1.02.32-1.el5

- Group: *System Environment/Base*
- Summary: *device mapper library*
- Description: *This package contains the supporting userspace files (libdevmapper and dmsetup) for the device-mapper.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-multipath-0.4.7-23.el5 - device-mapper-multipath-0.4.7-30.el5

- Group: *System Environment/Base*
- Summary: *Tools to manage multipath devices using device-mapper.*
- Description: *device-mapper-multipath provides tools to manage multipath devices by instructing the device-mapper multipath kernel module what to do. The tools are : * multipath : Scan the system for multipath devices and assemble them. * multipathd : Detects when paths fail and execs multipath to update things.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dhcp-3.0.5-18.el5 - dhcp-3.0.5-21.el5

- Group: *System Environment/Daemons*
- Summary: *DHCP (Dynamic Host Configuration Protocol) server and relay agent.*
- Description: *DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual*

devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network. The dhcp package includes the ISC DHCP service and relay agent. To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dhcpv6-1.0.10-16.el5 - dhcpv6-1.0.10-17.el5

- Group: *System Environment/Daemons*
- Summary: *DHCPv6 - DHCP server and client for IPv6*
- Description: *Implements the Dynamic Host Configuration Protocol (DHCP) for Internet Protocol version 6 (IPv6) networks in accordance with RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Consists of dhcp6s(8), the server DHCP daemon, and dhcp6r(8), the DHCPv6 relay agent. Install this package if you want to support dynamic configuration of IPv6 addresses and parameters on your IPv6 network.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dmidecode-2.7-1.28.2.el5 - dmidecode-2.9-1.el5

- Group: *System Environment/Base*
- Summary: *Tool to analyse BIOS DMI data.*
- Description: *dmidecode reports information about x86 hardware as described in the system BIOS according to the SMBIOS/DMI standard. This information typically includes system manufacturer, model name, serial number, BIOS version, asset tag as well as a lot of other details of varying level of interest and reliability depending on the manufacturer. This will often*

include usage status for the CPU sockets, expansion slots (e.g. AGP, PCI, ISA) and memory module slots, and the list of I/O ports (e.g. serial, parallel, USB).

- Added Dependencies:
  - automake
- Removed Dependencies:
  - /usr/bin/aclocal
  - /usr/bin/autoconf
  - /usr/bin/automake
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dmraid-1.0.0.rc13-33.el5 - dmraid-1.0.0.rc13-53.el5

- Group: *System Environment/Base*
- Summary: *dmraid (Device-mapper RAID tool and library)*
- Description: *DMRAID supports RAID device discovery, RAID set activation and display of properties for ATARAID on Linux >= 2.4 using device-mapper.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dos2unix-3.1-27.1 - dos2unix-3.1-27.2.el5

- Group: *Applications/Text*
- Summary: *Text file format converter*
- Description: *Dos2unix converts DOS or MAC text files to UNIX format.*
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dump-0.4b41-2.fc6 - dump-0.4b41-4.el5

- Group: *Applications/Archiving*
- Summary: *Programs for backing up and restoring ext2/ext3 filesystems*
- Description: *The dump package contains both dump and restore. Dump examines files in a filesystem, determines which ones need to be backed up, and copies those files to a specified disk, tape, or other storage medium. The restore command performs the inverse function of dump; it can restore a full backup of a filesystem. Subsequent incremental backups can then be layered on top of the full backup. Single files and directory subtrees may also be restored from full or partial backups. Install dump if you need a system for both backing up filesystems and restoring filesystems after backups.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dvd+rw-tools-7.0-0.el5.3 - dvd+rw-tools-7.0-1.el5

- Group: *Applications/Multimedia*
- Summary: *Toolchain to master DVD+RW/+R media*
- Description: *Collection of tools to master DVD+RW/+R media. For further information see http://fy.chalmers.se/~appro/linux/DVD+RW/.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

e2fsprogs-1.39-20.el5 - e2fsprogs-1.39-23.el5

- Group: *System Environment/Base*
- Summary: *Utilities for managing the second and third extended (ext2/ext3) filesystems*
- Description: *The e2fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in second and third extended (ext2/ext3) filesystems. E2fsprogs contains e2fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke2fs (used to initialize a partition to contain an empty ext2 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e2fsck), tune2fs (used to modify filesystem parameters), and most of the other core ext2fs filesystem utilities. You should install the e2fsprogs package if you need to manage the performance of an ext2 and/or ext3 filesystem.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

e4fsprogs-1.41.1-2.el5 - e4fsprogs-1.41.5-3.el5

- Group: *System Environment/Base*
- Summary: *Utilities for managing the fourth extended (ext4) filesystem*
- Description: *The e4fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the fourth extended (ext4) filesystem. E4fsprogs contains e4fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e4fsck), tune4fs (used to modify filesystem parameters), and most of the other core ext4fs filesystem utilities. Please note that "e4fsprogs" simply contains renamed static binaries from the equivalent upstream e2fsprogs release; it is packaged this way for Red Hat Enterprise Linux 5 to ensure that the many changes included for ext4 do not destabilize the core e2fsprogs in RHEL5. You should install the e4fsprogs package if you need to manage the performance of an ext4 filesystem.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ecryptfs-utils-56-8.el5 - ecryptfs-utils-75-5.el5

- Group: *System Environment/Base*
- Summary: *The eCryptfs mount helper and support libraries*
- Description: *eCryptfs is a stacked cryptographic filesystem that ships in the Linux kernel. This package provides the mount helper and supporting libraries to perform key management and mount functions. Install ecryptfs-utils if you would like to mount eCryptfs.*
- Added Dependencies:
  - nss-devel
  - python
  - python-devel
  - trousers-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

efax-0.9-27.2.1 - efax-0.9-28.el5

- Group: *Applications/Communications*
- Summary: *A program for faxing using a Class 1, 2 or 2.0 fax modem.*
- Description: *Efax is a small ANSI C/POSIX program that sends and receives faxes using any Class 1, 2 or 2.0 fax modem. You need to install efax if you want to send faxes and you have a Class 1, 2 or 2.0 fax modem.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

esc-1.0.0-39.el5 - esc-1.1.0-9.el5

- Group: *Applications/Internet*
- Summary: *Enterprise Security Client Smart Card Client*
- Description: *Enterprise Security Client allows the user to enroll and manage their cryptographic smartcards.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ethtool-6-2.el5 - ethtool-6-3.el5

- Group: *Applications/System*
- Summary: *Ethernet settings tool for PCI ethernet cards*
- Description: *This utility allows querying and changing of ethernet card settings, such as speed, port, autonegotiation, and PCI locations.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

evince-0.6.0-8.el5 - evince-0.6.0-9.el5

- Group: *Applications/Publishing*
- Summary: *Document viewer*
- Description: *evince is a GNOME-based document viewer.*

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

evolution-data-server-1.12.3-6.el5_2.3 - evolution-data-server-1.12.3-18.el5

- Group: *System Environment/Libraries*
- Summary: *Backend data server for Evolution*
- Description: *The evolution-data-server package provides a unified backend for programs that work with contacts, tasks, and calendar information. It was originally developed for Evolution (hence the name), but is now used by other packages.*
- Added Dependencies:
  - libXau-devel
  - xorg-x11-proto-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

file-4.17-15 - file-4.17-15.el5_3.1

- Group: *Applications/File*
- Summary: *A utility for determining file types.*
- Description: *The file command is used to identify a particular file according to the type of data contained by the file. File can identify many different file types, including ELF binaries, system libraries, RPM packages, and different graphics formats. You should install the file package, since the file command is such a useful utility.*
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

findutils-4.2.27-5.el5 - findutils-4.2.27-6.el5

- Group: *Applications/File*
- Summary: *The GNU versions of find utilities (find and xargs).*
- Description: *The findutils package contains programs which will help you locate files on your system. The find utility searches through a hierarchy of directories looking for files which match a certain set of criteria (such as a filename pattern). The xargs utility builds and executes command lines from standard input arguments (usually lists of file names generated by the find command). You should install findutils because it includes tools that are very useful for finding things on your system.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

fipscheck-1.0.3-1.el5 - fipscheck-1.2.0-1.el5

- Group: *System Environment/Libraries*
- Summary: *A library for integrity verification of FIPS validated modules*
- Description: *FIPSCheck is a library for integrity verification of FIPS validated modules. The package also provides helper binaries for creation and verification of the HMAC-SHA256 checksum files.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

firefox-3.0.5-1.el5_2 - firefox-3.0.12-1.el5_3

- Group: *Applications/Internet*
- Summary: *Mozilla Firefox Web browser*
- Description: *Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.*
- Added Dependencies:
  - xulrunner-devel >= 1.9.0.12-1
  - xulrunner-devel-unstable >= 1.9.0.12-1
- Removed Dependencies:
  - xulrunner-devel >= 1.9.0.5-1
  - xulrunner-devel-unstable >= 1.9.0.5-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

foomatic-3.0.2-38.1.el5 - foomatic-3.0.2-38.3.el5

- Group: *System Environment/Libraries*
- Summary: *Foomatic printer database.*
- Description: *Foomatic is a comprehensive, spooler-independent database of printers, printer drivers, and driver descriptions. It contains utilities to generate driver description files and printer queues for CUPS, LPD, LPRng, and PDQ using the database. There is also the possibility to read the PJL options out of PJL-capable laser printers and take them into account at the driver description file generation. There are spooler-independent command line interfaces to manipulate queues (foomatic-configure) and to print files/manipulate jobs (foomatic printjob). The site http://www.linuxprinting.org/ is based on this database.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

freetype-2.2.1-20.el5_2 - freetype-2.2.1-21.el5_3

- Group: *System Environment/Libraries*
- Summary: *A free and portable font rendering engine*
- Description: *The FreeType engine is a free and portable font rendering engine, developed to provide advanced font support for a variety of platforms and environments. FreeType is a library which can open and manages font files as well as efficiently load, hint and render individual glyphs. FreeType is not a font server or a complete text-rendering library.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc-4.1.2-44.el5 - gcc-4.1.2-46.el5

- Group: *Development/Languages*
- Summary: *Various compilers (C, C++, Objective-C, Java, ...)*
- Description: *The gcc package contains the GNU Compiler Collection version 4.1. You'll need this package in order to compile C code.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdb-6.8-27.el5 - gdb-6.8-37.el5

- Group: *Development/Debuggers*
- Summary: *A GNU source-level debugger for C, C++, Java and other languages*
- Description: *GDB, the GNU debugger, allows you to debug programs written in C, C++, Java, and other languages, by executing them in a controlled fashion and printing their data.*

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdm-2.16.0-46.el5 - gdm-2.16.0-56.el5

- Group: *User Interface/X*
- Summary: *The GNOME Display Manager.*
- Description: *Gdm (the GNOME Display Manager) is a highly configurable reimplementation of xdm, the X Display Manager. Gdm allows you to log into your system with the X Window System running and supports running several different X sessions on your local machine at the same time.*
- Added Dependencies:
  - tcp_wrappers
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs-kmod-0.1.31-3.el5 - gfs-kmod-0.1.34-2.el5

- Group: *System Environment/Kernel*
- Summary: *gfs kernel modules*
- Description: *gfs - The Global File System is a symmetric, shared-disk, cluster file system.*
- Added Dependencies:
  - kernel-devel-ia64 = 2.6.18-159.el5
  - kernel-xen-devel-ia64 = 2.6.18-159.el5
- Removed Dependencies:
  - kernel-devel-ia64 = 2.6.18-128.el5

- kernel-xen-devel-ia64 = 2.6.18-128.el5

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs-utils-0.1.18-1.el5 - gfs-utils-0.1.20-1.el5

- Group: *System Environment/Kernel*
- Summary: *Utilities for managing the global filesystem (GFS)*
- Description: *The gfs-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs2-utils-0.1.53-1.el5 - gfs2-utils-0.1.62-1.el5

- Group: *System Environment/Kernel*
- Summary: *Utilities for managing the global filesystem (GFS)*
- Description: *The gfs2-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ghostscript-8.15.2-9.4.el5 - ghostscript-8.15.2-9.11.el5

- Group: *Applications/Publishing*
- Summary: *A PostScript(TM) interpreter and renderer.*
- Description: *Ghostscript is a set of software that provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by your printer or screen. Ghostscript is normally used to display PostScript files and to print PostScript files to non-PostScript printers. If you need to display PostScript files or print them to non-PostScript printers, you should install ghostscript. If you install ghostscript, you also need to install the ghostscript-fonts package.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

giflib-4.1.3-7.1.el5.1 - giflib-4.1.3-7.1.el5_3.1

- Group: *System Environment/Libraries*
- Summary: *Library for manipulating GIF format image files*
- Description: *The giflib package contains a shared library of functions for loading and saving GIF format image files. It is API and ABI compatible with libungif, the library which supported uncompressed GIFs while the Unisys LZW patent was in effect. Install the giflib package if you need to write programs that use GIF files. You should also install the giflib-utils package if you need some simple utilities to manipulate GIFs.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

glib2-2.12.3-2.fc6 - glib2-2.12.3-4.el5_3.1

- Group: *System Environment/Libraries*

- Summary: *A library of handy utility functions*
- Description: *GLib is the 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. This package provides version 2 of GLib.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

glibc-2.5-34 - glibc-2.5-42

- Group: *System Environment/Libraries*
- Summary: *The GNU libc libraries.*
- Description: *The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-python2-desktop-2.16.0-2.el5 - gnome-python2-desktop-2.16.0-3.el5

- Group: *Development/Languages*
- Summary: *The sources for additional PyGNOME Python extension modules for the GNOME desktop*
- Description: *The gnome-python-desktop package contains the source packages for additional Python bindings for GNOME. It should be used together with gnome-python.*

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-session-2.16.0-6.el5 - gnome-session-2.16.0-7.el5

- Group: *User Interface/Desktops*
- Summary: *GNOME session manager*
- Description: *gnome-session manages a GNOME desktop session. It starts up the other core GNOME components and handles logout and saving the session.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

grep-2.5.1-54.2.el5 - grep-2.5.1-55.el5

- Group: *Applications/Text*
- Summary: *The GNU versions of grep pattern matching utilities.*
- Description: *The GNU versions of commonly used grep utilities. Grep searches through textual input for lines which contain a match to a specified pattern and then prints the matching lines. GNU's grep utilities include grep, egrep and fgrep. You should install grep on your system, because it is a very useful utility for searching through text.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

grub-0.97-13.2 - grub-0.97-13.5

- Group: *System Environment/Base*
- Summary: *GRUB - the Grand Unified Boot Loader.*
- Description: *GRUB (Grand Unified Boot Loader) is an experimental boot loader capable of booting into most free operating systems - Linux, FreeBSD, NetBSD, GNU Mach, and others as well as most commercial operating systems.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gstreamer-plugins-base-0.10.20-3.el5 - gstreamer-plugins-base-0.10.20-3.0.1.el5_3

- Group: *Applications/Multimedia*
- Summary: *GStreamer streaming media framework base plug-ins*
- Description: *GStreamer is a streaming media framework, based on graphs of filters which operate on media data. Applications using this library can do anything from real-time sound processing to playing videos, and just about anything else media-related. Its plugin-based architecture means that new data types or processing capabilities can be added simply by installing new plug-ins. This package contains a set of well-maintained base plug-ins.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gstreamer-plugins-good-0.10.9-1.el5 - gstreamer-plugins-good-0.10.9-1.el5_3.2

- Group: *Applications/Multimedia*

- Summary: *GStreamer plug-ins with good code and licensing*
- Description: *GStreamer is a streaming media framework, based on graphs of filters which operate on media data. Applications using this library can do anything from real-time sound processing to playing videos, and just about anything else media-related. Its plugin-based architecture means that new data types or processing capabilities can be added simply by installing new plug-ins. GStreamer Good Plug-ins is a collection of well-supported plug-ins of good quality and under the LGPL license.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk-vnc-0.3.2-3.el5 - gtk-vnc-0.3.8-3.el5

- Group: *Development/Libraries*
- Summary: *A GTK widget for VNC clients*
- Description: *gtk-vnc is a VNC viewer widget for GTK. It is built using coroutines allowing it to be completely asynchronous while remaining single threaded.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hal-0.5.8.1-38.el5 - hal-0.5.8.1-52.el5

- Group: *System Environment/Libraries*
- Summary: *Hardware Abstraction Layer*
- Description: *HAL is daemon for collection and maintaining information from several sources about the hardware on the system. It provides a live device list through D-BUS.*
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

htdig-3.2.0b6-9.0.1.el5_1 - htdig-3.2.0b6-11.el5

- Group: *Applications/Internet*
- Summary: *ht://Dig - Web search engine*
- Description: *The ht://Dig system is a complete world wide web indexing and searching system for a small domain or intranet. This system is not meant to replace the need for powerful internet-wide search systems like Lycos, Infoseek, Webcrawler and AltaVista. Instead it is meant to cover the search needs for a single company, campus, or even a particular sub section of a web site. As opposed to some WAIS-based or web-server based search engines, ht://Dig can span several web servers at a site. The type of these different web servers doesn't matter as long as they understand the HTTP 1.0 protocol. ht://Dig is also used by KDE to search KDE's HTML documentation. ht://Dig was developed at San Diego State University as a way to search the various web servers on the campus network.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

httpd-2.2.3-22.el5 - httpd-2.2.3-31.el5

- Group: *System Environment/Daemons*
- Summary: *Apache HTTP Server*
- Description: *The Apache HTTP Server is a powerful, efficient, and extensible web server.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

hwbrowser-0.30-2.el5 - hwbrowser-0.30-3.el5

- Group: *Applications/System*
- Summary: *A hardware browser.*
- Description: *A browser for your current hardware configuration.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hwdata-0.213.11-1.el5 - hwdata-0.213.16-1.el5

- Group: *System Environment/Base*
- Summary: *Hardware identification and configuration data*
- Description: *hwdata contains various hardware identification and configuration data, such as the pci.ids database and MonitorsDb databases.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ibsim-0.4-3.el5 - ibsim-0.5-1.el5

- Group: *System Environment/Libraries*
- Summary: *InfiniBand fabric simulator for management*
- Description: *ibsim provides simulation of infiniband fabric for using with OFA OpenSM, diagnostic and management tools.*

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ibutils-1.2-9.el5 - ibutils-1.2-10.el5

- Group: *System Environment/Libraries*
- Summary: *OpenIB Mellanox InfiniBand Diagnostic Tools*
- Description: *ibutils provides IB network and path diagnostics.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

icu-3.6-5.11.1 - icu-3.6-5.11.4

- Group: *System Environment/Libraries*
- Summary: *International Components for Unicode*
- Description: *The International Components for Unicode (ICU) libraries provide robust and full-featured Unicode services on a wide variety of platforms. ICU supports the most current version of the Unicode standard, and they provide support for supplementary Unicode characters (needed for GB 18030 repertoire support). As computing environments become more heterogeneous, software portability becomes more important. ICU lets you produce the same results across all the various platforms you support, without sacrificing performance. It offers great flexibility to extend and customize the supplied services.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

infiniband-diags-1.4.1-2.el5 - infiniband-diags-1.4.4-1.el5

- Group: *System Environment/Libraries*
- Summary: *OpenFabrics Alliance InfiniBand Diagnostic Tools*
- Description: *This package provides IB diagnostic programs and scripts needed to diagnose an IB subnet.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

initscripts-8.45.25-1.el5 - initscripts-8.45.30-2.el5

- Group: *System Environment/Base*
- Summary: *The inittab file and the /etc/init.d scripts.*
- Description: *The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also contains the scripts that activate and deactivate most network interfaces.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iproute-2.6.18-9.el5 - iproute-2.6.18-10.el5

- Group: *Applications/System*

- Summary: *Advanced IP routing and network device configuration tools.*
- Description: *The iproute package contains networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux 2.4.x and 2.6.x kernel.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iprutils-2.2.8-2.el5 - iprutils-2.2.13-1.el5

- Group: *System Environment/Base*
- Summary: *Utilities for the IBM Power Linux RAID adapters*
- Description: *Provides a suite of utilities to manage and configure SCSI devices supported by the ipr SCSI storage device driver.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipsec-tools-0.6.5-13.el5 - ipsec-tools-0.6.5-13.el5_3.1

- Group: *System Environment/Base*
- Summary: *Tools for configuring and using IPSEC*
- Description: *This is the IPsec-Tools package. You need this package in order to really use the IPsec functionality in the linux-2.5+ kernels. This package builds: - setkey, a program to directly manipulate policies and SAs - racoon, an IKEv1 keying daemon*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iptables-1.3.5-4.el5 - iptables-1.3.5-5.3.el5

- Group: *System Environment/Base*
- Summary: *Tools for managing Linux kernel packet filtering capabilities.*
- Description: *The iptables utility controls the network packet filtering code in the Linux kernel. If you need to set up firewalls and/or IP masquerading, you should install this package.*
- Added Dependencies:
  - kernel-headers >= 2.6.18-141.el5
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iputils-20020927-45.el5 - iputils-20020927-46.el5

- Group: *System Environment/Daemons*
- Summary: *Network monitoring tools including ping.*
- Description: *The iputils package contains basic utilities for monitoring a network, including ping. The ping command sends a series of ICMP protocol ECHO_REQUEST packets to a specified network host to discover whether the target machine is alive and receiving network traffic.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipvsadm-1.24-8.1 - ipvsadm-1.24-10

- Group: *Applications/System*
- Summary: *Utility to administer the Linux Virtual Server*
- Description: *ipvsadm is a utility to administer the IP Virtual Server services offered by the Linux kernel.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

irqbalance-0.55-10.el5 - irqbalance-0.55-15.el5

- Group: *System Environment/Base*
- Summary: *IRQ balancing daemon.*
- Description: *irqbalance is a daemon that evenly distributes IRQ load across multiple CPUs for enhanced performance.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iscsi-initiator-utils-6.2.0.868-0.18.el5 - iscsi-initiator-utils-6.2.0.871-0.10.el5

- Group: *System Environment/Daemons*
- Summary: *iSCSI daemon and utility programs*
- Description: *The iscsi package provides the server daemon for the 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.*
- Added Dependencies:
  - doxygen
  - python-devel

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

isdn4k-utils-3.2-51.el5 - isdn4k-utils-3.2-56.el5

- Group: *Applications/System*
- Summary: *Utilities for configuring an ISDN subsystem.*
- Description: *The isdn4k-utils package contains a collection of utilities needed for configuring an ISDN subsystem.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

jadetex-3.12-13.1.1 - jadetex-3.12-15.el5

- Group: *Applications/Publishing*
- Summary: *TeX macros used by Jade TeX output.*
- Description: *JadeTeX contains the additional LaTeX macros necessary for taking Jade TeX output files and processing them as TeX files (to obtain DVI, PostScript, or PDF files, for example).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-0.25.b09.el5 - java-1.6.0-openjdk-1.6.0.0-1.2.b09.el5

- Group: *Development/Languages*
- Summary: *OpenJDK Runtime Environment*
- Description: *The OpenJDK runtime environment.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdebase-3.5.4-19.el5 - kdebase-3.5.4-20.el5

- Group: *User Interface/Desktops*
- Summary: *K Desktop Environment - core files*
- Description: *Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdelibs-3.5.4-18.el5 - kdelibs-3.5.4-22.el5_3

- Group: *System Environment/Libraries*
- Summary: *K Desktop Environment - Libraries*

- Description: *Libraries for the K Desktop Environment: KDE Libraries included: kdecore (KDE core library), kdeui (user interface), kfm (file manager), khtmlw (HTML widget), kio (Input/Output, networking), kspell (spelling checker), jscript (javascript), kab (addressbook), kimgio (image manipulation).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdenetwork-3.5.4-8.el5 - kdenetwork-3.5.4-9.el5

- Group: *Applications/Internet*
- Summary: *K Desktop Environment - Network Applications*
- Description: *Networking applications for the K Desktop Environment.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kernel-2.6.18-128.el5 - kernel-2.6.18-164.el5

- Group: *System Environment/Kernel*
- Summary: *The Linux kernel (the core of the Linux operating system)*
- Description: *The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.*
- Added Dependencies:
  - hmaccalc
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kexec-tools-1.102pre-56.el5 - kexec-tools-1.102pre-77.el5

- Group: *Applications/System*
- Summary: *The kexec/kdump userspace component.*
- Description: *kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

krb5-1.6.1-31.el5 - krb5-1.6.1-36.el5

- Group: *System Environment/Libraries*
- Summary: *The Kerberos network authentication system.*
- Description: *Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ksh-20080202-2.el5 - ksh-20080202-14.el5

- Group: *Applications/Shells*
- Summary: *The Original ATT Korn Shell*
- Description: *KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language, which is upward compatible with "sh" (the Bourne Shell).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lcms-1.15-1.2.2 - lcms-1.18-0.1.beta1.el5_3.2

- Group: *Applications/Productivity*
- Summary: *Color Management System*
- Description: *LittleCMS intends to be a small-footprint, speed optimized color management engine in open source form.*
- Added Dependencies:
  - autoconf
  - automake
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

less-394-5.el5 - less-394-6.el5

- Group: *Applications/Text*
- Summary: *A text file browser similar to more, but better.*
- Description: *The less utility is a text file browser that resembles more, but has more capabilities.*

Less allows you to move backwards in the file as well as forwards. Since less doesn't have to read the entire input file before it starts, less starts up more quickly than text editors (for example, vi). You should install less because it is a basic utility for viewing text files, and you'll use it frequently.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lftp-3.5.1-2.fc6 - lftp-3.7.11-4.el5

- Group: *Applications/Internet*
- Summary: *A sophisticated file transfer program*
- Description: *LFTP is a sophisticated ftp/http file transfer program. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.*
- Added Dependencies:
  - gnutls-devel
- Removed Dependencies:
  - openssl-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libX11-1.0.3-9.el5 - libX11-1.0.3-11.el5

- Group: *System Environment/Libraries*
- Summary: *X.Org X11 libX11 runtime library*
- Description: *X.Org X11 libX11 runtime library*
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcxgb3-1.2.2-1.el5 - libcxgb3-1.2.3-1.el5

- Group: *System Environment/Libraries*
- Summary: *Chelsio T3 iWARP HCA Userspace Driver*
- Description: *Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- Removed Dependencies:
  - libibverbs-devel >= 1.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libdhcp-1.20-6.el5 - libdhcp-1.20-10.el5

- Group: *Development/Libraries*
- Summary: *A library for network interface configuration with DHCP*
- Description: *libdhcp enables programs to invoke and control the Dynamic Host Configuration Protocol (DHCP) clients: the Internet Software Consortium (ISC) IPv4 DHCP client library, libdhcp4client, and the IPv6 DHCPv6 client library, libdhcp6client, and provides Network Interface Configuration (NIC) services for network parameter autoconfiguration with DHCP.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

libehca-1.2-2.el5 - libehca-1.2.1-3.el5

- Group: *System Environment/Libraries*
- Summary: *IBM InfiniBand HCA Userspace Driver*
- Description: *IBM hardware driver for use with libibverbs user space verbs access library.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4
- Removed Dependencies:
  - libibverbs-devel >= 1.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libgcrypt-1.2.4-1.el5 - libgcrypt-1.4.4-5.el5

- Group: *System Environment/Libraries*
- Summary: *A general-purpose cryptography library*
- Description: *Libgcrypt is a general purpose crypto library based on the code used in GNU Privacy Guard. This is a development version.*
- Added Dependencies:
  - fipscheck
  - gawk
  - libgpg-error-devel >= 1.4
- Removed Dependencies:
  - libgpg-error-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

libibcm-1.0.3-1.el5 - libibcm-1.0.4-3.el5

- Group: *System Environment/Libraries*
- Summary: *Userspace InfiniBand Communication Manager.*
- Description: *libibcm provides a userspace InfiniBand Communication Managment library.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- Removed Dependencies:
  - libibverbs-devel >= 1.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibcommon-1.1.1-1.el5 - libibcommon-1.1.2-1.el5

- Group: *System Environment/Libraries*
- Summary: *OpenFabrics Alliance InfiniBand management common library*
- Description: *libibcommon provides common utility functions for the OFA diagnostic and management tools.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibmad-1.2.1-1.el5 - libibmad-1.2.3-1.el5

- Group: *System Environment/Libraries*
- Summary: *OpenFabrics Alliance InfiniBand MAD library*
- Description: *libibmad provides low layer IB functions for use by the IB diagnostic and management programs. These include MAD, SA, SMP, and other basic IB functions.*

- Added Dependencies:
  - libibumad-devel >= 1.2.3
- Removed Dependencies:
  - libibumad-devel >= 1.2.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibumad-1.2.1-1.el5 - libibumad-1.2.3-1.el5

- Group: *System Environment/Libraries*
- Summary: *OpenFabrics Alliance InfiniBand umad (user MAD) library*
- Description: *libibumad provides the user MAD library functions which sit on top of the user MAD modules in the kernel. These are used by the IB diagnostic and management tools, including OpenSM.*
- Added Dependencies:
  - libibcommon-devel >= 1.1.2
- Removed Dependencies:
  - libibcommon-devel >= 1.1.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibverbs-1.1.2-1.el5 - libibverbs-1.1.2-4.el5

- Group: *System Environment/Libraries*
- Summary: *Library providing access to InfiniBand/iWARP hardware verbs protocol*
- Description: *libibverbs is a library that allows userspace processes to use InfiniBand/iWARP "verbs" as described in the InfiniBand Architecture Specification. This includes direct hardware access for fast path operations. For this library to be useful, a device-specific plug-in module should also be installed.*
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libipathverbs-1.1-11.el5 - libipathverbs-1.1-14.el5

- Group: *System Environment/Libraries*
- Summary: *QLogic InfiniPath HCA Userspace Driver*
- Description: *QLogic hardware driver for use with libibverbs user space verbs access library. This driver supports QLogic InfiniPath based cards.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
  - valgrind
- Removed Dependencies:
  - libibverbs-devel >= 1.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmlx4-1.0-4.el5 - libmlx4-1.0.1-2.el5

- Group: *System Environment/Libraries*
- Summary: *Mellanox ConnectX InfiniBand HCA Userspace Driver*
- Description: *Mellanox hardware driver for use with libibverbs user space verbs access library. This driver supports Mellanox ConnectX architecture cards.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- Removed Dependencies:
  - libibverbs-devel >= 1.1
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmthca-1.0.5-1.el5 - libmthca-1.0.5-4.el5

- Group: *System Environment/Libraries*
- Summary: *Mellanox InfiniBand HCA Userspace Driver*
- Description: *Mellanox hardware driver for use with libibverbs user space verbs access library. This driver supports Mellanox based Single Data Rate and Dual Data Rate cards, including those from Cisco, Topspin, and Voltaire. It does not support the Connect-X architecture based Quad Data Rate cards (libmlx4 handles that hardware).*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- Removed Dependencies:
  - libibverbs-devel >= 1.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libnes-0.5-4.el5 - libnes-0.6-2.el5

- Group: *System Environment/Libraries*
- Summary: *NetEffect RNIC Userspace Driver*
- Description: *Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables NetEffect iWARP capable ethernet devices.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- Removed Dependencies:
  - libibverbs-devel >= 1.1
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

libpng-1.2.10-7.1.el5_0.1 - libpng-1.2.10-7.1.el5_3.2

- Group: *System Environment/Libraries*
- Summary: *A library of functions for manipulating PNG image format files*
- Description: *The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files. PNG is a bit-mapped graphics format similar to the GIF format. PNG was created to replace the GIF format, since GIF uses a patented data compression algorithm. Libpng should be installed if you need to manipulate PNG format image files.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

librdmacm-1.0.8-1.el5 - librdmacm-1.0.8-5.el5

- Group: *System Environment/Libraries*
- Summary: *Userspace RDMA Connection Manager.*
- Description: *librdmacm provides a userspace RDMA Communication Managment API.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- Removed Dependencies:
  - libibverbs-devel >= 1.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libsdp-1.1.99-10.el5_2 - libsdp-1.1.99-11.el5

- Group: *System Environment/Libraries*
- Summary: *A library for direct userspace use of Sockets Direct Protocol*
- Description: *libsdp is an LD_PRELOAD-able library that can be used to have existing applications use InfiniBand Sockets Direct Protocol (SDP) instead of TCP sockets, transparently and without recompilation. For information on how to configure libsdp, see libsdp.conf, which is installed in $(sysconfdir) (usually /usr/local/etc or /etc).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libselinux-1.33.4-5.1.el5 - libselinux-1.33.4-5.5.el5

- Group: *System Environment/Libraries*
- Summary: *SELinux library and simple utilities*
- Description: *Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. libselinux provides an API for SELinux applications to get and set process and file security contexts and to obtain security policy decisions. Required for any applications that use the SELinux API.*
- Added Dependencies:
  - ruby
  - ruby-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libsemanage-1.9.1-3.el5 - libsemanage-1.9.1-4.4.el5

- Group: *System Environment/Libraries*
- Summary: *SELinux binary policy manipulation library*
- Description: *Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. libsemanage provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, as well as by programs like load_policy that need to perform specific transformations on binary policies such as customizing policy boolean settings.*
- Added Dependencies:
  - libsepol-devel >= 1.15.2-2
- Removed Dependencies:
  - libsepol-devel >= 1.14-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libsepol-1.15.2-1.el5 - libsepol-1.15.2-2.el5

- Group: *System Environment/Libraries*
- Summary: *SELinux binary policy manipulation library*
- Description: *Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. libsepol provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, as well as by programs like load_policy that need to perform specific transformations on binary policies such as customizing policy boolean settings.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libsoup-2.2.98-2.el5 - libsoup-2.2.98-2.el5_3.1

- Group: *Development/Libraries*
- Summary: *Soup, an HTTP library implementation*
- Description: *Libsoup is an HTTP library implementation in C. It was originally part of a SOAP (Simple Object Access Protocol) implementation called Soup, but the SOAP and non-SOAP parts have now been split into separate packages. libsoup uses the Glib main loop and is designed to work well with GTK applications. This enables GNOME applications to access HTTP servers on the network in a completely asynchronous fashion, very similar to the Gtk+ programming model (a synchronous operation mode is also supported for those who want it).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libspe2-2.2.80.121-4.el5 - libspe2-2.3.0.135-3.el5

- Group: *System Environment/Base*
- Summary: *SPE Runtime Management Library*
- Description: *SPE Runtime Management Library for the Cell Broadband Engine Architecture.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtiff-3.8.2-7.el5_2.2 - libtiff-3.8.2-7.el5_3.4

- Group: *System Environment/Libraries*
- Summary: *Library of functions for manipulating TIFF format image files*
- Description: *The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large. The libtiff package should be installed if you need to manipulate TIFF format image files.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libunwind-0.98.5-3 - libunwind-0.98.5-5.el5

- Group: *Development/Debuggers*
- Summary: *An unwinding library for ia64.*
- Description: *Libunwind provides a C ABI to determine the call-chain of a program. This version of libunwind is targetted for the ia64 platform.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-0.3.3-14.el5 - libvirt-0.6.3-20.el5

- Group: *Development/Libraries*
- Summary: *Library providing a simple API virtualization*
- Description: *Libvirt is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).*
- Added Dependencies:
  - /usr/sbin/qcow-create

    - cyrus-sasl-devel
    - e2fsprogs-devel
    - gawk
    - hal-devel
    - iscsi-initiator-utils
    - libselinux-devel
    - lvm2
    - nfs-utils
    - numactl-devel
    - parted-devel
    - util-linux
    - xhtml1-dtds
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-cim-0.5.1-4.el5 - libvirt-cim-0.5.5-2.el5

- Group: *Development/Libraries*
- Summary: *A CIM provider for libvirt*
- Description: *Libvirt-cim is a CMPI CIM provider that implements the DMTF SVPC virtualization model. The goal is to support most of the features exported by libvirt itself, enabling management of multiple platforms with a single provider.*
- Added Dependencies:
    - libvirt-devel >= 0.6.3
- Removed Dependencies:
    - libvirt-devel >= 0.3.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

libvorbis-1.1.2-3.el5_1.2 - libvorbis-1.1.2-3.el5_3.3

- Group: *System Environment/Libraries*
- Summary: *The Vorbis General Audio Compression Codec.*
- Description: *Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format for audio and music at fixed and variable bitrates from 16 to 128 kbps/channel. The libvorbis package contains runtime libraries for use in programs that support Ogg Voribs.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libwmf-0.2.8.4-10.1 - libwmf-0.2.8.4-10.2

- Group: *System Environment/Libraries*
- Summary: *Windows Metafile Library*
- Description: *A library for reading and converting Windows MetaFile vector graphics (WMF)*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libxml2-2.6.26-2.1.2.7 - libxml2-2.6.26-2.1.2.8

- Group: *Development/Libraries*
- Summary: *Library providing XML and HTML support*
- Description: *This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even*

with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI library.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

linuxwacom-0.7.8.3-5.el5 - linuxwacom-0.7.8.3-6.el5

- Group: *User Interface/X Hardware Support*
- Summary: *Wacom Drivers from Linux Wacom Project*
- Description: *The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lksctp-tools-1.0.6-1.el5.1 - lksctp-tools-1.0.6-3.el5

- Group: *System Environment/Libraries*
- Summary: *User-space access to Linux Kernel SCTP*
- Description: *This is the lksctp-tools package for Linux Kernel SCTP (Stream Control Transmission Protocol) Reference Implementation. This package is intended to supplement the Linux Kernel SCTP Reference Implementation now available in the Linux kernel source tree in versions 2.5.36 and following. For more information on LKSCTP see the package documentation README file, section titled "LKSCTP - Linux Kernel SCTP." This package contains the base run-time library and command-line tools.*
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ltrace-0.5-7.45svn.el5 - ltrace-0.5-13.45svn.el5

- Group: *Development/Debuggers*
- Summary: *Tracks runtime library calls from dynamically linked executables.*
- Description: *Ltrace is a debugging program which runs a specified command until the command exits. While the command is executing, ltrace intercepts and records both the dynamic library calls called by the executed process and the signals received by the executed process. Ltrace can also intercept and print system calls executed by the process. You should install ltrace if you need a sysadmin tool for tracking the execution of processes.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-2.02.40-6.el5 - lvm2-2.02.46-8.el5

- Group: *System Environment/Base*
- Summary: *Userland logical volume management tools*
- Description: *LVM2 includes all of the support for handling read/write operations on physical volumes (hard disks, RAID-Systems, magneto optical, etc., multiple devices (MD), see mdadd(8) or even loop devices, see losetup(8)), creating volume groups (kind of virtual disks) from one or more physical volumes and creating one or more logical volumes (kind of logical partitions) in volume groups.*
- Added Dependencies:
  - device-mapper >= 1.02.32-1
- Removed Dependencies:
  - device-mapper >= 1.02.28-2

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-cluster-2.02.40-7.el5 - lvm2-cluster-2.02.46-8.el5

- Group: *System Environment/Base*
- Summary: *Cluster extensions for userland logical volume management tools*
- Description: *Extensions to LVM2 to support clusters.*
- Added Dependencies:
  - device-mapper >= 1.02.32-1
- Removed Dependencies:
  - device-mapper >= 1.02.28-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

m2crypto-0.16-6.el5.3 - m2crypto-0.16-6.el5.6

- Group: *System Environment/Libraries*
- Summary: *Support for using OpenSSL in python scripts*
- Description: *This package allows you to call OpenSSL functions from python scripts.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-ja-20060815-9.el5 - man-pages-ja-20060815-11.el5

- Group: *Documentation*
- Summary: *Japanese man (manual) pages from the Japanese Manual Project*
- Description: *Japanese Manual pages, translated by JM-Project (Japanese Manual Project).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mcelog-0.7-1.22.fc6 - mcelog-0.9pre-1.27.el5

- Group: *System Environment/Base*
- Summary: *Tool to translate x86-64 CPU Machine Check Exception data.*
- Description: *mcelog is a daemon that collects and decodes Machine Check Exception data on x86-64 machines.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mdadm-2.6.4-1.el5 - mdadm-2.6.9-2.el5

- Group: *System Environment/Base*
- Summary: *mdadm controls Linux md devices (software RAID arrays)*
- Description: *mdadm is used to create, manage, and monitor Linux MD (software RAID) devices. As such, it provides similar functionality to the raidtools package. However, mdadm is a single program, and it can perform almost all functions without a configuration file, though a configuration file can be used to help with some common tasks.*
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

microcode_ctl-1.17-1.47.el5 - microcode_ctl-1.17-1.48.el5

- Group: *System Environment/Base*
- Summary: *Tool to update x86/x86-64 CPU microcode.*
- Description: *microcode_ctl - updates the microcode on Intel x86/x86-64 CPU's*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mkinitrd-5.1.19.6-44 - mkinitrd-5.1.19.6-54

- Group: *System Environment/Base*
- Summary: *Creates an initial ramdisk image for preloading modules.*
- Description: *Mkinitrd creates filesystem images for use as initial ramdisk (initrd) images. These ramdisk images are often used to preload the block device modules (SCSI or RAID) needed to access the root filesystem. In other words, generic kernels can be built without drivers for any SCSI adapters which load the SCSI driver as a module. Since the kernel needs to read those modules, but in this case it isn't able to address the SCSI adapter, an initial ramdisk is used. The initial ramdisk is loaded by the operating system loader (normally LILO) and is available to the kernel as soon as the ramdisk is loaded. The ramdisk image loads the proper SCSI adapter and allows the kernel to mount the root filesystem. The mkinitrd program creates such a ramdisk using information found in the /etc/modules.conf file.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

mlocate-0.15-1.el5.1 - mlocate-0.15-1.el5.2

- Group: *Applications/System*
- Summary: *An utility for finding files by name*
- Description: *mlocate is a locate/updatedb implementation. It keeps a database of all existing files and allows you to lookup files by name. The 'm' stands for "merging": updatedb reuses the existing database to avoid rereading most of the file system, which makes updatedb faster and does not trash the system caches as much as traditional locate implementations.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_auth_mysql-3.0.0-3.1 - mod_auth_mysql-3.0.0-3.2.el5_3

- Group: *System Environment/Daemons*
- Summary: *Basic authentication for the Apache web server using a MySQL database.*
- Description: *mod_auth_mysql can be used to limit access to documents served by a web server by checking data in a MySQL database.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_authz_ldap-0.26-8.el5 - mod_authz_ldap-0.26-9.el5

- Group: *System Environment/Daemons*
- Summary: *LDAP authorization module for the Apache HTTP Server*

- Description: *The mod_authz_ldap package provides support for authenticating users of the Apache HTTP server against an LDAP database. mod_authz_ldap features the ability to authenticate users based on the SSL client certificate presented, and also supports password aging, and authentication based on role or by configured filters.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_nss-1.0.3-6.el5 - mod_nss-1.0.3-8.el5

- Group: *System Environment/Daemons*
- Summary: *SSL/TLS module for the Apache HTTP server*
- Description: *The mod_nss module provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols using the Network Security Services (NSS) security library.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

module-init-tools-3.3-0.pre3.1.42.el5 - module-init-tools-3.3-0.pre3.1.54.el5

- Group: *System Environment/Kernel*
- Summary: *Kernel module management utilities.*
- Description: *The modutils package includes various programs needed for automatic loading and unloading of modules under 2.6 and later kernels, as well as other module management programs. Device drivers and filesystems are two examples of loaded and unloaded modules.*
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mpi-selector-1.0.1-1.el5 - mpi-selector-1.0.2-1.el5

- Group: *System Environment/Base*
- Summary: *Provides site-wide and per-user MPI implementation selection*
- Description: *A simple tool that allows system administrators to set a site-wide default for which MPI implementation is to be used, but also allow users to set their own default MPI implementation, thereby overriding the site-wide default. The default can be changed easily via the mpi-selector command -- editing of shell startup files is not required.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mpitests-3.0-2.el5 - mpitests-3.1-3.el5

- Group: *Applications*
- Summary: *MPI Benchmarks and tests*
- Description: *Set of popular MPI benchmarks: IMB-2.3 Presta-1.4.0 OSU benchmarks ver 2.2*
- Added Dependencies:
  - mvapich >= 1.1.0-0.3355.2
  - mvapich2 >= 1.2-0.p1.3
  - openmpi >= 1.3.2-2
- Removed Dependencies:
  - libibcommon-devel
  - libibumad-devel
  - libibverbs-devel

    - mvapich
    - mvapich2
    - openmpi
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

mstflint-1.3-1.el5 - mstflint-1.4-1.el5

  - Group: *Applications/System*
  - Summary: *Mellanox firmware burning tool*
  - Description: *This package contains a burning tool for Mellanox manufactured HCA cards. It also provides access to the relevant source code.*
  - No added dependencies
  - No removed dependencies
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

mvapich-1.1.0-0.2931.3.el5 - mvapich-1.1.0-0.3355.2.el5

  - Group: *Development/Libraries*
  - Summary: *MPI implementation over Infiniband RDMA-enabled interconnect*
  - Description: *This is high performance and scalable MPI-1 implementation over Infiniband and RDMA-enabled interconnects. This implementation is based on MPICH and MVICH. MVAPICH is pronounced as `em-vah-pich".*
  - Added Dependencies:
    - autoconf
    - libibverbs-devel >= 1.1.2-4.el5
  - Removed Dependencies:
    - libibverbs-devel

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mvapich2-1.0.3-3.el5 - mvapich2-1.2-0.p1.3.el5

- Group: *Development/Libraries*
- Summary: *OSU MVAPICH2 MPI package*
- Description: *This is an MPI-2 implementation which includes all MPI-1 features. It is based on MPICH2 and MVICH.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- Removed Dependencies:
  - libibverbs-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mysql-5.0.45-7.el5 - mysql-5.0.77-3.el5

- Group: *Applications/Databases*
- Summary: *MySQL client programs and shared libraries*
- Description: *MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the MySQL client programs, the client shared libraries, and generic MySQL files.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

mysql-connector-odbc-3.51.12-2.2 - mysql-connector-odbc-3.51.26r1127-1.el5

- Group: *System Environment/Libraries*
- Summary: *ODBC driver for MySQL*
- Description: *An ODBC (rev 3) driver for MySQL, for use with unixODBC.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

net-snmp-5.3.2.2-5.el5 - net-snmp-5.3.2.2-7.el5

- Group: *System Environment/Daemons*
- Summary: *A collection of SNMP protocol tools and libraries.*
- Description: *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, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmptrapd daemons, documentation, etc. You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities. Building option: --without tcp_wrappers : disable tcp_wrappers support*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

netpbm-10.35-6.fc6 - netpbm-10.35.58-8.el5

- Group: *System Environment/Libraries*

- Group: *System Environment/Libraries*
- Summary: *A library for handling different graphics file formats*
- Description: *The netpbm package contains a library of functions which support programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps) and others.*
- Added Dependencies:
  - python
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-1.0.9-40.el5 - nfs-utils-1.0.9-42.el5

- Group: *System Environment/Daemons*
- Summary: *NFS utilities and supporting clients and daemons for the kernel NFS server.*
- Description: *The nfs-utils package provides a daemon for the kernel NFS server and related tools, which provides a much higher level of performance than the traditional Linux NFS server used by most users. This package also contains the showmount program. Showmount queries the mount daemon on a remote host for information about the NFS (Network File System) server on the remote host. For example, showmount can display the clients which are mounted on that host. This package also contains the mount.nfs and umount.nfs program.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-lib-1.0.8-7.2.z2 - nfs-utils-lib-1.0.8-7.6.el5

- Group: *System Environment/Libraries*
- Summary: *Network File System Support Library*
- Description: *Support libraries that are needed by the commands and daemons the nfs-utils rpm.*

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs4-acl-tools-0.3.1-1.el5.1 - nfs4-acl-tools-0.3.3-1.el5

- Group: *System Environment/Tools*
- Summary: *The nfs4 ACL tools*
- Description: *This package contains commandline and GUI ACL utilities for the Linux NFSv4 client.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nspr-4.7.3-2.el5 - nspr-4.7.4-1.el5_3.1

- Group: *System Environment/Libraries*
- Summary: *Netscape Portable Runtime*
- Description: *NSPR provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing and calendar time, basic memory management (malloc and free) and shared library linking.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

nss-3.12.2.0-2.el5 - nss-3.12.3.99.3-1.el5_3.2

- Group: *System Environment/Libraries*
- Summary: *Network Security Services*
- Description: *Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss_ldap-253-17.el5 - nss_ldap-253-21.el5

- Group: *System Environment/Base*
- Summary: *NSS library and PAM module for LDAP.*
- Description: *This package includes two LDAP access clients: nss_ldap and pam_ldap. Nss_ldap is a set of C library extensions that allow X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Pam_ldap is a module for Linux-PAM that supports password changes, V2 clients, Netscape's SSL, ypldapd, Netscape Directory Server password policies, access authorization, and crypted hashes.*
- No added dependencies
- Removed Dependencies:
  - fipscheck-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

ntp-4.2.2p1-9.el5 - ntp-4.2.2p1-9.el5_3.2

- Group: *System Environment/Daemons*
- Summary: *Synchronizes system time using the Network Time Protocol (NTP).*
- Description: *The Network Time Protocol (NTP) is used to synchronize a computer's time with another reference time source. The ntp package contains utilities and daemons that will synchronize your computer's time to Coordinated Universal Time (UTC) via the NTP protocol and NTP servers. The ntp package includes ntpdate (a program for retrieving the date and time from remote machines via a network) and ntpd (a daemon which continuously adjusts system time). Install the ntp package if you need tools for keeping your system's time synchronized via the NTP protocol.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

numactl-0.9.8-7.el5 - numactl-0.9.8-8.el5

- Group: *System Environment/Base*
- Summary: *library for tuning for Non Uniform Memory Access machines*
- Description: *Simple NUMA policy support. It consists of a numactl program to run other programs with a specific NUMA policy and a libnuma to do allocations with NUMA policy in applications.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ofed-docs-1.3.2-0.20080728.0355.1.el5 - ofed-docs-1.4.1-2.el5

- Group: *Documentation/Man*

- Summary: *OpenFabrics Enterprise Distribution documentation*
- Description: *Documentation from OFED 1.3*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openais-0.80.3-22.el5 - openais-0.80.6-8.el5

- Group: *System Environment/Base*
- Summary: *The openais Standards-Based Cluster Framework executive and APIs*
- Description: *This package contains the openais executive, openais service handlers, default configuration files and init script.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openhpi-2.10.2-1.el5 - openhpi-2.14.0-5.el5

- Group: *System Environment/Base*
- Summary: *openhpi Hardware Platform Interface (HPI) library and tools*
- Description: *OpenHPI is an open source project created with the intent of providing an implementation of the SA Forum's Hardware Platform Interface (HPI). HPI provides an abstracted interface to managing computer hardware, typically for chassis and rack based servers. HPI includes resource modeling; access to and control over sensor, control, watchdog, and inventory data associated with resources; abstracted System Event Log interfaces; hardware events and alerts; and a managed hotswap interface. OpenHPI provides a modular mechanism for adding new hardware and device support easily. Many plugins exist in the OpenHPI source tree to provide access to various types of hardware. This includes, but is not limited to, IPMI based servers, Blade Center, and machines which export data via sysfs.*
- Added Dependencies:

    - docbook-utils
    - libxml2-devel
  - No removed dependencies
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

openib-1.3.2-0.20080728.0355.3.el5 - openib-1.4.1-3.el5

  - Group: *System Environment/Base*
  - Summary: *OpenIB Infiniband Driver Stack*
  - Description: *User space initialization scripts for the kernel InfiniBand drivers*
  - No added dependencies
  - No removed dependencies
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

openmpi-1.2.7-6.el5 - openmpi-1.3.2-2.el5

  - Group: *Development/Libraries*
  - Summary: *Open Message Passing Interface*
  - Description: *Open MPI is an open source, freely available implementation of both the MPI-1 and MPI-2 standards, combining technologies and resources from several other projects (FT-MPI, LA-MPI, LAM/MPI, and PACX-MPI) in order to build the best MPI library available. A completely new MPI-2 compliant implementation, Open MPI offers advantages for system and software vendors, application developers, and computer science researchers. For more information, see http://www.open-mpi.org/ .*
  - Added Dependencies:
    - compat-dapl-devel >= 2.0.19-2
    - libibverbs-devel >= 1.1.2-4
  - Removed Dependencies:

    - compat-dapl-devel
    - libibverbs-devel
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

opensm-3.2.2-3.el5 - opensm-3.2.6-2.el5

  - Group: *System Environment/Daemons*
  - Summary: *OpenIB InfiniBand Subnet Manager and management utilities*
  - Description: *OpenSM is the OpenIB project's Subnet Manager for Infiniband networks. The subnet manager is run as a system daemon on one of the machines in the infiniband fabric to manage the fabric's routing state. This package also contains various tools for diagnosing and testing Infiniband networks that can be used from any machine and do not need to be run on a machine running the opensm daemon.*
  - Added Dependencies:
    - libibmad-devel >= 1.2.3
  - Removed Dependencies:
    - libibmad-devel >= 1.2.1
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

openssh-4.3p2-29.el5 - openssh-4.3p2-36.el5

  - Group: *Applications/Internet*
  - Summary: *The OpenSSH implementation of SSH protocol versions 1 and 2*
  - Description: *SSH (Secure SHell) is a program for logging into and executing commands on a remote machine. SSH is intended to replace rlogin and rsh, and to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. OpenSSH is OpenBSD's version of the last free version of SSH, bringing it up to date in terms of security and features, as well as removing all patented algorithms to separate libraries. This package includes the core files necessary for both the OpenSSH client and server. To make this package useful, you should also install openssh-clients, openssh-server, or both.*

- Added Dependencies:
  - fipscheck-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssl-0.9.8e-7.el5 - openssl-0.9.8e-12.el5

- Group: *System Environment/Libraries*
- Summary: *The OpenSSL toolkit*
- Description: *The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.*
- No added dependencies
- Removed Dependencies:
  - fipscheck
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openswan-2.6.14-1.el5_2.1 - openswan-2.6.21-5.el5

- Group: *System Environment/Daemons*
- Summary: *Openswan IPSEC implementation*
- Description: *Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN. This package contains the daemons and userland tools for setting up Openswan. It optionally also builds the Openswan KLIPS IPsec stack that is an alternative for the NETKEY/XFRM IPsec stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4309)*

- Added Dependencies:
  - bind-devel
  - fipscheck-devel >= 1.2.0-1
  - nss-devel >= 3.12.3-2
  - xmlto
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

oprofile-0.9.3-18.el5 - oprofile-0.9.4-11.el5

- Group: *Development/System*
- Summary: *System wide profiler*
- Description: *OProfile is a profiling system for systems running Linux. The profiling runs transparently during the background, and profile data can be collected at any time. OProfile makes use of the hardware performance counters provided on Intel P6, and AMD Athlon family processors, and can use the RTC for profiling on other x86 processor types. See the HTML documentation for further details.*
- Added Dependencies:
  - libtool
  - popt
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pam-0.99.6.2-4.el5 - pam-0.99.6.2-6.el5

- Group: *System Environment/Base*
- Summary: *A security tool which provides authentication for applications*
- Description: *PAM (Pluggable Authentication Modules) is a system security tool that allows*

system administrators to set authentication policy without having to recompile programs that handle authentication.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pango-1.14.9-3.el5 - pango-1.14.9-6.el5

- Group: *System Environment/Libraries*
- Summary: *System for layout and rendering of internationalized text*
- Description: *Pango is a system for layout and rendering of internationalized text.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pciutils-2.2.3-5 - pciutils-2.2.3-7.el5

- Group: *Applications/System*
- Summary: *PCI bus related utilities.*
- Description: *The pciutils package contains various utilities for inspecting and setting devices connected to the PCI bus. The utilities provided require kernel version 2.1.82 or newer (which support the /proc/bus/pci interface).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

perftest-1.2-11.el5 - perftest-1.2-14.el5

- Group: *Productivity/Networking/Diagnostic*
- Summary: *IB Performance tests*
- Description: *gen2 uverbs microbenchmarks*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4
  - librdmacm-devel >= 1.0.8-5
- Removed Dependencies:
  - libibverbs-devel
  - librdmacm-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-5.8.8-18.el5 - perl-5.8.8-27.el5

- Group: *Development/Languages*
- Summary: *The Perl programming language*
- Description: *Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.*
- No added dependencies
- Removed Dependencies:
  - gawk
  - grep
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-DBD-Pg-1.49-2.el5 - perl-DBD-Pg-1.49-2.el5_3.1

- Group: *Development/Libraries*
- Summary: *A PostgresSQL interface for perl*
- Description: *An implementation of DBI for PostgreSQL for Perl.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-5.1.6-23.el5 - php-5.1.6-23.2.el5_3

- Group: *Development/Languages*
- Summary: *The PHP HTML-embedded scripting language. (PHP: Hypertext Preprocessor)*
- Description: *PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-pear-1.4.9-4.el5.1 - php-pear-1.4.9-6.el5

- Group: *System*
- Summary: *PHP Extension and Application Repository framework*
- Description: *PEAR is a framework and distribution system for reusable PHP components. This package contains the basic PEAR components.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

piranha-0.8.4-11.el5 - piranha-0.8.4-13.el5

- Group: *System Environment/Base*
- Summary: *Cluster administation tools*
- Description: *Various tools to administer and configure the Linux Virtual Server as well as heartbeating and failover components. The LVS is a dynamically adjusted kernel routing mechanism that provides load balancing primarily for web and ftp servers though other services are supported.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

policycoreutils-1.33.12-14.2.el5 - policycoreutils-1.33.12-14.6.el5

- Group: *System Environment/Base*
- Summary: *SELinux policy core utilities.*
- Description: *Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide*

general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. policycoreutils contains the policy core utilities that are required for basic operation of a SELinux system. These utilities include load_policy to load policies, setfiles to label filesystems, newrole to switch roles, and run_init to run /etc/init.d scripts in the proper context.

- Added Dependencies:
  - libsemanage-devel >= 1.9.1-4.2
- Removed Dependencies:
  - libsemanage-devel >= 1.6.17-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

poppler-0.5.4-4.4.el5_1 - poppler-0.5.4-4.4.el5_3.9

- Group: *Development/Libraries*
- Summary: *PDF rendering library*
- Description: *Poppler, a PDF rendering library, it's a fork of the xpdf PDF viewer developed by Derek Noonburg of Glyph and Cog, LLC.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ppc64-utils-0.11-10.el5 - ppc64-utils-0.11-12.el5

- Group: *System Environment/Base*
- Summary: *Linux/PPC64 specific utilities*
- Description: *A collection of utilities for Linux on PPC64 platforms.*
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

psmisc-22.2-6 - psmisc-22.2-7

- Group: *Applications/System*
- Summary: *Utilities for managing processes on your system.*
- Description: *The psmisc package contains utilities for managing processes on your system: pstree, killall and fuser. The pstree command displays a tree structure of all of the running processes on your system. The killall command sends a specified signal (SIGTERM if nothing is specified) to processes identified by name. The fuser command identifies the PIDs of processes that are using specified files or filesystems.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pykickstart-0.43.3-1.el5 - pykickstart-0.43.5-1.el5

- Group: *System Environment/Libraries*
- Summary: *A python library for manipulating kickstart files*
- Description: *The pykickstart package is a python library for manipulating kickstart files.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

pyorbit-2.14.1-1.1 - pyorbit-2.14.1-3.el5

- Group: *Development/Languages*
- Summary: *Python bindings for ORBit2.*
- Description: *pyorbit is an extension module for python that gives you access to the ORBit2 CORBA ORB.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-2.4.3-24.el5 - python-2.4.3-27.el5

- Group: *Development/Languages*
- Summary: *An interpreted, interactive, object-oriented programming language.*
- Description: *Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs package.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-pyblock-0.26-3.el5 - python-pyblock-0.26-4.el5

- Group: *System Environment/Libraries*

- Summary: *Python modules for dealing with block devices*
- Description: *The pyblock contains Python modules for dealing with block devices.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-virtinst-0.300.2-12.el5 - python-virtinst-0.400.3-5.el5

- Group: *Development/Libraries*
- Summary: *Python modules and utilities for installing virtual machines*
- Description: *virtinst is a module that helps build and install libvirt based virtual machines. Currently supports KVM, QEmu and Xen virtual machines. Package includes several command line utilities, including virt-install (build and install new VMs) and virt-clone (clone an existing virtual machine).*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qlvnictools-0.0.1-10.el5 - qlvnictools-0.0.1-11.el5

- Group: *System Environment/Base*
- Summary: *VNIC ULP service*
- Description: *VNIC ULP service*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qperf-0.4.1-2.el5 - qperf-0.4.4-3.el5

- Group: *Networking/Diagnostic*
- Summary: *Measure socket and RDMA performance*
- Description: *Measure socket and RDMA performance.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4
  - librdmacm-devel >= 1.0.8-5
- Removed Dependencies:
  - libibverbs-devel
  - librdmacm-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rdesktop-1.4.1-6 - rdesktop-1.6.0-3

- Group: *User Interface/Desktops*
- Summary: *X client for remote desktop into Windows Terminal Server*
- Description: *rdesktop is an open source client for Windows NT Terminal Server and Windows 2000 & 2003 Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required.*
- Added Dependencies:
  - pcsc-lite-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

readline-5.1-1.1 - readline-5.1-3.el5

- Group: *System Environment/Libraries*
- Summary: *A library for editing typed command lines.*
- Description: *The Readline library provides a set of functions that allow users to edit command lines. Both Emacs and vi editing modes are available. The Readline library includes additional functions for maintaining a list of previously-entered command lines for recalling or editing those lines, and for performing csh-like history expansion on previous commands.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-5Server-5.3.0.3 - redhat-release-5Server-5.4.0.3

- Group: *System Environment/Base*
- Summary: *Red Hat Enterprise Linux release file*
- Description: *Red Hat Enterprise Linux release files*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-notes-5Server-25 - redhat-release-notes-5Server-29

- Group: *System Environment/Base*
- Summary: *Red Hat Enterprise Linux release notes files*
- Description: *Red Hat Enterprise Linux release notes files.*

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-rpm-config-8.0.45-29.el5 - redhat-rpm-config-8.0.45-32.el5

- Group: *Development/System*
- Summary: *Red Hat specific rpm configuration files.*
- Description: *Red Hat specific rpm configuration files.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rgmanager-2.0.46-1.el5 - rgmanager-2.0.52-1.el5

- Group: *System Environment/Base*
- Summary: *Open Source HA Resource Group Failover for Red Hat Enterprise Linux*
- Description: *Red Hat Resource Group Manager provides high availability of critical server applications in the event of planned or unplanned system downtime.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

rhn-client-tools-0.4.19-17.el5 - rhn-client-tools-0.4.20-9.el5

- Group: *System Environment/Base*
- Summary: *Support programs and libraries for Red Hat Network*
- Description: *Red Hat Network Client Tools provides programs and libraries to allow your system to receive software updates from Red Hat Network.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnlib-2.2.6-2.el5 - rhnlib-2.2.7-2.el5

- Group: *Development/Libraries*
- Summary: *Python libraries for the RHN project*
- Description: *rhnlib is a collection of python modules used by the Red Hat Network (http://rhn.redhat.com) software.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnsd-4.6.1-1.el5 - rhnsd-4.7.0-4.el5

- Group: *System Environment/Base*
- Summary: *Red Hat Network query daemon*
- Description: *The Red Hat Update Agent that automatically queries the Red Hat Network servers and determines which packages need to be updated on your machine, and runs any actions.*
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rpm-4.4.2.3-9.el5 - rpm-4.4.2.3-18.el5

- Group: *System Environment/Base*
- Summary: *The RPM package management system*
- Description: *The RPM Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Each software package consists of an archive of files along with information about the package like its version, a description, etc.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsh-0.17-38.el5 - rsh-0.17-40.el5

- Group: *Applications/Internet*
- Summary: *Clients for remote access commands (rsh, rlogin, rcp).*
- Description: *The rsh package contains a set of programs which allow users to run commands on remote machines, login to other machines and copy files between machines (rsh, rlogin and rcp). All three of these commands use rhosts style authentication. This package contains the clients needed for all of these services. The rsh package should be installed to enable remote access to other machines.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

ruby-1.8.5-5.el5_2.6 - ruby-1.8.5-5.el5_3.7

- Group: *Development/Languages*
- Summary: *An interpreter of object-oriented scripting language*
- Description: *Ruby is the interpreted scripting language for quick and easy object-oriented programming. It has many features to process text files and to do system management tasks (as in Perl). It is simple, straight-forward, and extensible.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

s390utils-1.5.3-21.el5 - s390utils-1.8.1-8.el5

- Group: *System Environment/Base*
- Summary: *Linux/390 specific utilities*
- Description: *This package contains utilities related to Linux for S/390. The most important programs contained in this package are: - The cmstools suite to list, check, copy and cat files from a CMS volume. - chccwdev, a script to generically change attributes of a ccw device. - dasdfmt, which is used to low-level format eckd-dasds with either the classic linux disk layout or the new z/OS compatible disk layout. - dasdview, which displays DASD and VTOC information and dumps the content of a DASD to the console. - fdasd, which is used to create or modify partitions on eckd-dasds formatted with the z/OS compatible disk layout. - osasnmpd, a subagent for net-snmp to access the OSA hardware. - qetharp to query and purge address data in the OSA and HiperSockets hardware - qethconf to configure IBM QETH function IPA, VIPA and Proxy ARP. - src_vipa.sh to start applications using VIPA capabilities - tunedasd, a tool to adjust tunable parameters on DASD devices - vmconvert, a tool to convert vm dumps to lkcd compatible dumps. - vmcp, a tool to send CP commands from a Linux guest to the VM. - vmur, a tool to work with z/VM spool file queues (reader, punch, printer). - zipl, which is used to make either dasds or tapes bootable for system IPL or system dump. - zdump, which is used to retrieve system dumps from either tapes or dasds. - ziomon tools to collect data for zfcp performance analysis and report. - iucvterm, a z/VM IUCV terminal applications. - cpuplugd, a daemon that manages CPU and memory resources based on a set of rules. - dumpconf, the dump device used for system dump in case a kernel panic occurs. - mon_statd, pair of Linux - z/VM monitoring daemons. - ipl_tools, tool set to configure and list reipl and shutdown actions.*
- Added Dependencies:
  - gettext

- Removed Dependencies:
  - indent
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

samba-3.0.33-3.7.el5 - samba-3.0.33-3.14.el5

- Group: *System Environment/Daemons*
- Summary: *The Samba SMB server.*
- Description: *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). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB server that can be used to provide network services to SMB (sometimes called "Lan Manager") clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sblim-1-31.el5_2.1 - sblim-1-35.el5

- Group: *Applications/System*
- Summary: *Standards Based Linux Instrumentation for Manageability*
- Description: *SBLIM stands for Standards Based Linux Instrumentation for Manageability, and consists of a set of standards based Web Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.*
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scim-bridge-0.4.5-8.el5 - scim-bridge-0.4.5-9.el5

- Group: *System Environment/Libraries*
- Summary: *SCIM Bridge Gtk IM module*
- Description: *SCIM Bridge is a C implementation of a Gtk IM module for SCIM.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

selinux-policy-2.4.6-203.el5 - selinux-policy-2.4.6-255.el5

- Group: *System Environment/Base*
- Summary: *SELinux policy configuration*
- Description: *SELinux Reference Policy - modular.*
- Added Dependencies:
  - policycoreutils >= 1.33.12-14.5
- Removed Dependencies:
  - policycoreutils >= 1.33.12-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

setroubleshoot-2.0.5-3.el5 - setroubleshoot-2.0.5-5.el5

- Group: *Applications/System*
- Summary: *Helps troubleshoot SELinux problems*
- Description: *setroubleshoot gui. Application that allows you to view setroubleshoot-server messages. Provides tools to help diagnose SELinux problems. When AVC messages are generated an alert can be generated that will give information about the problem and help track its resolution. Alerts can be configured to user preference. The same tools can be run on existing log files.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

setup-2.5.58-4.el5 - setup-2.5.58-7.el5

- Group: *System Environment/Base*
- Summary: *A set of system configuration and setup files.*
- Description: *The setup package contains a set of important system configuration and setup files, such as passwd, group, and profile.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sg3_utils-1.25-1.el5 - sg3_utils-1.25-4.el5

- Group: *Utilities/System*
- Summary: *Utils for Linux's SCSI generic driver devices + raw devices*
- Description: *Collection of Linux utilities for devices that use the SCSI command set. Includes*

utilities to copy data based on "dd" syntax and semantics (called sg_dd, sgp_dd and sgm_dd); check INQUIRY data and VPD pages (sg_inq); check mode and log pages (sginfo, sg_modes and sg_logs); spin up and down disks (sg_start); do self tests (sg_senddiag); and various other functions. See the README, CHANGELOG and COVERAGE files. Requires the linux kernel 2.4 series or later. In the 2.4 series SCSI generic device names (e.g. /dev/sg0) must be used. In the 2.6 series other device names may be used as well (e.g. /dev/sda). Warning: Some of these tools access the internals of your system and the incorrect usage of them may render your system inoperable.

- No added dependencies
- Removed Dependencies:
  - libtool
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sos-1.7-9.16.el5 - sos-1.7-9.27.el5

- Group: *Development/Libraries*
- Summary: *A set of tools to gather troubleshooting information from a system*
- Description: *Sos is a set of tools that gathers information about system hardware and configuration. The information can then be used for diagnostic purposes and debugging. Sos is commonly used to help support technicians and developers.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sqlite-3.3.6-2 - sqlite-3.3.6-5

- Group: *Applications/Databases*
- Summary: *Library that implements an embeddable SQL database engine*
- Description: *SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and*

flexibility of an SQL database without the administrative hassles of supporting a separate database server. Version 2 and version 3 binaries are named to permit each to be installed on a single host

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

squirrelmail-1.4.8-4.0.1.el5 - squirrelmail-1.4.8-5.el5_3.7

- Group: *Applications/Internet*
- Summary: *SquirrelMail webmail client*
- Description: *SquirrelMail is a standards-based webmail package written in PHP4. It includes built-in pure PHP support for the IMAP and SMTP protocols, and all pages render in pure HTML 4.0 (with no Javascript) for maximum compatibility across browsers. It has very few requirements and is very easy to configure and install. SquirrelMail has all the functionality you would want from an email client, including strong MIME support, address books, and folder manipulation.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

srptools-0.0.4-2.el5 - srptools-0.0.4-6.el5

- Group: *System Environment/Base*
- Summary: *Tools for using the InfiniBand SRP protocol devices*
- Description: *In conjunction with the kernel ib_srp driver, srptools allows you to discover and use SCSI devices via the SCSI RDMA Protocol over InfiniBand.*
- Added Dependencies:
  - libibverbs-devel >= 1.1.2-4

- Removed Dependencies:
  - libibverbs-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

strace-4.5.18-2.el5 - strace-4.5.18-5.el5

- Group: *Development/Debuggers*
- Summary: *Tracks and displays system calls associated with a running process*
- Description: *The strace program intercepts and records the system calls called and received by a running process. Strace can print a record of each system call, its arguments and its return value. Strace is useful for diagnosing problems and debugging, as well as for instructional purposes. Install strace if you need a tool to track the system calls made and received by a process.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subversion-1.4.2-4.el5 - subversion-1.4.2-4.el5_3.1

- Group: *Development/Tools*
- Summary: *Modern Version Control System designed to replace CVS*
- Description: *Subversion 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. Subversion only stores the differences between versions, instead of every complete file. Subversion is intended to be a compelling replacement for CVS.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sudo-1.6.9p17-3.el5 - sudo-1.6.9p17-5.el5

- Group: *Applications/System*
- Summary: *Allows restricted root access for specified users.*
- Description: *Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis, copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.*
- Added Dependencies:
  - sendmail
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-cluster-1.0.55-1.0 - system-config-cluster-1.0.57-1.5

- Group: *Applications/System*
- Summary: *system-config-cluster is a utility which allows you to manage cluster configuration in a graphical setting.*
- Description: *system-config-cluster is a utility which allows you to manage cluster configuuration in a graphical setting.*
- Added Dependencies:
  - intltool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-date-1.8.12-3.el5 - system-config-date-1.8.12-4.el5

- Group: *System Environment/Base*
- Summary: *A graphical interface for modifying system date and time*
- Description: *system-config-date is a graphical interface for changing the system date and time, configuring the system time zone, and setting up the NTP daemon to synchronize the time of the system with an NTP time server.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-language-1.1.18-2.el5 - system-config-language-1.1.18-3.el5

- Group: *System Environment/Base*
- Summary: *A graphical interface for modifying the system language*
- Description: *system-config-language is a graphical user interface that allows the user to change the default language of the system.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-network-1.3.99.12-1.el5 - system-config-network-1.3.99.18-1.el5

- Group: *Applications/System*
- Summary: *The GUI of the NEtwork Adminstration Tool*

- Description: *This is the GUI of the network configuration tool, supporting Ethernet, Wireless, TokenRing, ADSL, ISDN and PPP.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-samba-1.2.41-3.el5 - system-config-samba-1.2.41-5.el5

- Group: *System Environment/Base*
- Summary: *Samba server configuration tool*
- Description: *system-config-samba is a graphical user interface for creating, modifying, and deleting samba shares.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

systemtap-0.7.2-2.el5 - systemtap-0.9.7-5.el5

- Group: *Development/System*
- Summary: *Instrumentation System*
- Description: *SystemTap is an instrumentation system for systems running Linux 2.6. Developers can write instrumentation to collect data on the operation of the system.*
- Added Dependencies:
  - /usr/share/xmlto/format/fo/pdf
  - m4
  - nss-devel
  - xmlto

- Removed Dependencies:
  - elfutils-devel >= 0.127
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tcl-8.4.13-3.fc6 - tcl-8.4.13-4.el5

- Group: *Development/Languages*
- Summary: *Tcl scripting language development environment*
- Description: *The Tcl (Tool Command Language) provides a powerful platform for creating integration applications that tie together diverse applications, protocols, devices, and frameworks. When paired with the Tk toolkit, Tcl provides a fastest and powerful way to create cross-platform GUI applications. Tcl can also be used for a variety of web-related tasks and for creating powerful command languages for applications.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tcp_wrappers-7.6-40.6.el5 - tcp_wrappers-7.6-40.7.el5

- Group: *System Environment/Daemons*
- Summary: *A security tool which acts as a wrapper for TCP daemons.*
- Description: *The tcp_wrappers package provides small daemon programs which can monitor and filter incoming requests for systat, finger, FTP, telnet, rlogin, rsh, exec, tftp, talk and other network services. Install the tcp_wrappers program if you need a security tool for filtering incoming network services requests. This version also supports IPv6.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tetex-3.0-33.2.el5_1.2 - tetex-3.0-33.8.el5

- Group: *Applications/Publishing*
- Summary: *The TeX text formatting system.*
- Description: *TeTeX is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a typesetter-independent .dvi (DeVice Independent) file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX, since TeX by itself is not very user-friendly. The output format needn't to be DVI, but also PDF, when using pdflatex or similar tools. Install tetex if you want to use the TeX text formatting system. Consider to install tetex-latex (a higher level formatting package which provides an easier-to-use interface for TeX). Unless you are an expert at using TeX, you should also install the tetex-doc package, which includes the documentation for TeX.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tftp-0.42-3.1 - tftp-0.49-2

- Group: *Applications/Internet*
- Summary: *The client for the Trivial File Transfer Protocol (TFTP).*
- Description: *The Trivial File Transfer Protocol (TFTP) is normally used only for booting diskless workstations. The tftp package provides the user interface for TFTP, which allows users to transfer files to and from a remote machine. This program and TFTP provide very little security, and should not be enabled unless it is expressly needed.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

tog-pegasus-2.7.1-2.el5 - tog-pegasus-2.7.2-1.el5

- Group: *Systems Management/Base*
- Summary: *OpenPegasus WBEM Services for Linux*
- Description: *OpenPegasus WBEM Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent DMTF standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tomcat5-5.5.23-0jpp.7.el5_2.1 - tomcat5-5.5.23-0jpp.7.el5_3.2

- Group: *Networking/Daemons*
- Summary: *Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API*
- Description: *Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

totem-2.16.7-4.el5 - totem-2.16.7-6.el5

- Group: *Applications/Multimedia*
- Summary: *Movie player for GNOME 2*
- Description: *Totem is simple movie player for the Gnome desktop. It features a simple playlist, a full-screen mode, seek and volume controls, as well as a pretty complete keyboard navigation.*
- Added Dependencies:
  - gstreamer-plugins-good >= 0.10.0
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tzdata-2008i-1.el5 - tzdata-2009k-1.el5

- Group: *System Environment/Base*
- Summary: *Timezone data*
- Description: *This package contains data files with rules for various timezones around the world.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

udev-095-14.19.el5 - udev-095-14.21.el5

- Group: *System Environment/Base*
- Summary: *A userspace implementation of devfs*
- Description: *The udev package contains an implementation of devfs in userspace using sysfs and netlink.*
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

unix2dos-2.2-26.2.2 - unix2dos-2.2-26.2.3.el5

- Group: *Applications/Text*
- Summary: *unix2dos - UNIX to DOS text file format converter*
- Description: *A utility that converts plain text files in UNIX format to DOS format.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

util-linux-2.13-0.50.el5 - util-linux-2.13-0.52.el5

- Group: *System Environment/Base*
- Summary: *A collection of basic system utilities.*
- Description: *The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login program.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vim-7.0.109-4.el5_2.4z - vim-7.0.109-6.el5

- Group: *Applications/Editors*
- Summary: *The VIM editor.*
- Description: *VIM (VIsual editor iMproved) is an updated and improved version of the vi editor. Vi was the first real screen-based editor for UNIX, and is still very popular. VIM improves on vi by adding new features: multiple windows, multi-level undo, block highlighting and more.*
- Added Dependencies:
  - ncurses-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vino-2.13.5-6.el5 - vino-2.13.5-7.el5

- Group: *User Interface/Desktops*
- Summary: *A remote desktop system for GNOME*
- Description: *Vino is a VNC server for GNOME. It allows remote users to connect to a running GNOME session using VNC.*
- Added Dependencies:
  - autoconf
  - automake
  - gnutls-devel
  - intltool
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

virt-manager-0.5.3-10.el5 - virt-manager-0.6.1-8.el5

- Group: *Applications/Emulators*
- Summary: *Virtual Machine Manager*
- Description: *Virtual Machine Manager provides a graphical tool for administering virtual machines for KVM, Xen, and QEmu. Start, stop, add or remove virtual devices, connect to a graphical or serial console, and see resource usage statistics for existing VMs on local or remote machines. Uses libvirt as the backend management API.*
- Added Dependencies:
  - atk-devel
  - cairo-devel
  - glib2-devel
  - intltool
  - pango-devel
  - pygobject2-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

virt-viewer-0.0.2-2.el5 - virt-viewer-0.0.2-3.el5

- Group: *Applications/System*
- Summary: *Virtual Machine Viewer*
- Description: *Virtual Machine Viewer provides a graphical console client for connecting to virtual machines. It uses the GTK-VNC widget to provide the display, and libvirt for looking up VNC server details.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vnc-4.1.2-14.el5 - vnc-4.1.2-14.el5_3.1

- Group: *User Interface/Desktops*
- Summary: *A remote display system.*
- Description: *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. This package contains a client which will allow you to connect to other desktops running a VNC server.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vsftpd-2.0.5-12.el5 - vsftpd-2.0.5-16.el5

- Group: *System Environment/Daemons*
- Summary: *vsftpd - Very Secure Ftp Daemon*
- Description: *vsftpd is a Very Secure FTP daemon. It was written completely from scratch.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

watchdog-5.3.1-7.el5 - watchdog-5.6-1.el5

- Group: *System Environment/Daemons*
- Summary: *Software and/or Hardware watchdog daemon*
- Description: *The watchdog program can be used as a powerful software watchdog daemon or may be alternately used with a hardware watchdog device such as the IPMI hardware watchdog driver interface to a resident Baseboard Management Controller (BMC). watchdog periodically writes to /dev/watchdog; the interval between writes to /dev/watchdog is configurable through settings in the watchdog sysconfig file. This configuration file is also used*

to set the watchdog to be used as a hardware watchdog instead of its default software watchdog operation. In either case, if the device is open but not written to within the configured time period, the watchdog timer expiration will trigger a machine reboot. When operating as a software watchdog, the ability to reboot will depend on the state of the machine and interrupts. When operating as a hardware watchdog, the machine will experience a hard reset (or whatever action was configured to be taken upon watchdog timer expiration) initiated by the BMC.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wdaemon-0.14-2 - wdaemon-0.14-4

- Group: *User Interface/X Hardware Support*
- Summary: *Hotplug helper for Wacom X.org driver*
- Description: *Helper application which emulates persistent input devices for Wacom tablets so they can be plugged and unplugged while X.org server is running. This should go away as soon X.org properly supports hotplugging.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wget-1.10.2-7.el5 - wget-1.11.4-2.el5

- Group: *Applications/Internet*
- Summary: *A utility for retrieving files using the HTTP or FTP protocols.*
- Description: *GNU Wget is a file retrieval utility which can use either the HTTP or FTP protocols. Wget features include the ability to work in the background while you are logged out, recursive retrieval of directories, file name wildcard matching, remote file timestamp storage and comparison, use of Rest with FTP servers and Range with HTTP servers to retrieve files over slow or unstable connections, support for Proxy servers, and configurability.*

- Added Dependencies:
  - zlib-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wireshark-1.0.3-4.el5_2 - wireshark-1.0.8-1.el5_3.1

- Group: *Applications/Internet*
- Summary: *Network traffic analyzer*
- Description: *Wireshark is a network traffic analyzer for Unix-ish operating systems. This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, contains plugins and documentation for wireshark. A graphical user interface is packaged separately to GTK+ package.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xen-3.0.3-80.el5 - xen-3.0.3-94.el5

- Group: *Development/Libraries*
- Summary: *Xen is a virtual machine monitor*
- Description: *This package contains the Xen tools and management daemons needed to run virtual machines on x86, x86_64, and ia64 systems. Information on how to use Xen can be found at the Xen project pages. The Xen system also requires the Xen hypervisor and domain-0 kernel, which can be found in the kernel-xen* package. Virtualization can be used to run multiple operating systems on one physical system, for purposes of hardware consolidation, hardware abstraction, or to test untrusted applications in a sandboxed environment.*
- Added Dependencies:
  - pciutils-devel

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xkeyboard-config-0.8-7.fc6 - xkeyboard-config-0.8-9.el5

- Group: *User Interface/X*
- Summary: *xkeyboard-config alternative xkb data files*
- Description: *xkeyboard-config alternative xkb data files*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-ati-6.6.3-3.22.el5 - xorg-x11-drv-ati-6.6.3-3.27.el5

- Group: *User Interface/X Hardware Support*
- Summary: *Xorg X11 ati video driver*
- Description: *X.Org X11 ati video driver.*
- Added Dependencies:
  - xorg-x11-server-sdk >= 1.1.1-48.58.el5
- Removed Dependencies:
  - xorg-x11-server-randr-source >= 1.1.1-48.52.el5
  - xorg-x11-server-sdk >= 1.1.1-24
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

xorg-x11-drv-i810-1.6.5-9.21.el5 - xorg-x11-drv-i810-1.6.5-9.25.el5

- Group: *User Interface/X Hardware Support*
- Summary: *Xorg X11 i810 video driver(s)*
- Description: *X.Org X11 i810 video driver.*
- Added Dependencies:
  - xorg-x11-server-sdk >= 1.1.1-48.58.el5
- Removed Dependencies:
  - xorg-x11-server-randr-source >= 1.1.1-48.46.el5
  - xorg-x11-server-sdk >= 1.1.0-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-mga-1.4.2-10.el5 - xorg-x11-drv-mga-1.4.10-5.el5

- Group: *User Interface/X Hardware Support*
- Summary: *Xorg X11 mga video driver*
- Description: *X.Org X11 mga video driver.*
- Added Dependencies:
  - xorg-x11-server-sdk >= 1.1.1-48.64.el5
- Removed Dependencies:
  - xorg-x11-server-sdk >= 1.1.0-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-nv-2.1.12-3.el5 - xorg-x11-drv-nv-2.1.12-6.el5

- Group: *User Interface/X Hardware Support*
- Summary: *Xorg X11 nv video driver*
- Description: *X.Org X11 nv video driver.*
- Added Dependencies:
  - xorg-x11-server-sdk >= 1.1.1-48.58.el5
- Removed Dependencies:
  - xorg-x11-server-randr-source >= 1.1.1-48.46.el5
  - xorg-x11-server-sdk >= 1.1.1-48.22
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-proto-devel-7.1-9.fc6 - xorg-x11-proto-devel-7.1-13.el5

- Group: *Development/System*
- Summary: *X.Org X11 Protocol headers*
- Description: *X.Org X11 Protocol headers*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-server-1.1.1-48.52.el5 - xorg-x11-server-1.1.1-48.67.el5

- Group: *User Interface/X*
- Summary: *X.Org X11 X server*
- Description: *X.Org X11 X server*
- Added Dependencies:
  - xorg-x11-proto-devel >= 7.1-13.el5

- Removed Dependencies:
  - xorg-x11-proto-devel >= 7.1-8
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xulrunner-1.9.0.5-1.el5_2 - xulrunner-1.9.0.12-1.el5_3

- Group: *Applications/Internet*
- Summary: *XUL Runtime for Gecko Applications*
- Description: *XULRunner provides the XUL Runtime environment for Gecko applications.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yaboot-1.3.13-7.el5 - yaboot-1.3.13-8.el5

- Group: *System Environment/Base*
- Summary: *Linux bootloader for Power Macintosh "New World" computers.*
- Description: *yaboot is a bootloader for PowerPC machines which works on New World ROM machines (Rev. A iMac and newer) and runs directly from Open Firmware, eliminating the need for Mac OS. yaboot can also bootload IBM pSeries machines.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

ypbind-1.19-11.el5 - ypbind-1.19-12.el5

- Group: *System Environment/Daemons*
- Summary: *The NIS daemon which binds NIS clients to an NIS domain.*
- Description: *The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in on any machine on the network, as long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP). This package provides the ypbind daemon. The ypbind daemon binds NIS clients to an NIS domain. Ypbind must be running on any machines running NIS client programs. Install the ypbind package on any machines running NIS client programs (included in the yp-tools package). If you need an NIS server, you also need to install the ypserv package to a machine on your network.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-3.2.19-18.el5 - yum-3.2.22-20.el5

- Group: *System Environment/Base*
- Summary: *RPM installer/updater*
- Description: *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 as necessary.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-metadata-parser-1.1.2-2.el5 - yum-metadata-parser-1.1.2-3.el5

- Group: *Development/Libraries*
- Summary: *A fast metadata parser for yum*
- Description: *Fast metadata parser for yum implemented in C.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-rhn-plugin-0.5.3-30.el5 - yum-rhn-plugin-0.5.4-13.el5

- Group: *System Environment/Base*
- Summary: *RHN support for yum*
- Description: *This yum plugin provides support for yum to access a Red Hat Network server for software updates.*
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zsh-4.2.6-1 - zsh-4.2.6-3.el5

- Group: *System Environment/Shells*
- Summary: *A powerful interactive shell*
- Description: *The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.*
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

Appendix B. Revision History

Revision 1-3.402	**Fri Oct 25 2013**	**Rüdiger Landmann**
Rebuild with Publican 4.0.0		
Revision 1-3	**Thu Jan 12 2012**	**Martin Prpic**
Removed an obsolete known issue note. BZ#625275		
Revision 1-1	**Thu Sep 03 2009**	**Ryan Lerch**
Added the Preface, Updated the Abstract, and corrected erroneous errata IDs		
Revision 1-0	**Wed Sep 02 2009**	**Ryan Lerch**
Initial Release of the Technical Notes		