Insecurity News

rlpr

rlpr makes it possible to print files on remote sites to your local printer.

jaguar@felinemenace.org has discovered a format string vulnerability in rlpr. While investigating this flaw, a buffer overflow was also discovered in related code. By exploiting one of these vulnerabilities, a local or remote user could potentially cause arbitrary code to be executed with the privileges of 1) the rlprd process (remote), or 2) root (local).

The first error is a format string vulnerability via syslog(3) in msg() function in rlpr. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0393 to this issue.

The other error is a buffer overflow in the msg() function in rlpr. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0454 to this issue. ■

Debian reference DSA-524-1 rlpr -- several vulnerabilities

Webmin

Webmin is an interface for system administration. Using a browser that supports tables and forms you can setup user accounts, Apache, DNS and so on.

A bug in Webmin 1.140 allows remote attackers to bypass access control rules and gain read access to configuration information. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0582 to this issue.

The account lockout functionality in (1) Webmin 1.140 and (2) Usermin 1.070 does not parse certain character strings, which allows remote attackers to conduct a brute force attack to guess user IDs and passwords. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0583 to this issue. ■

Debian reference DSA-526-1 webmin -- several vulnerabilities

Gentoo reference GLSA 200406-12 / Webmin

Security Posture of Major Distributions

Distributor	Security Sources	Comments
Debian	Info: *http://www.debian.org/security/* List: *http://lists.debian.org/debian-security-announce/* Reference: DSA-... 1)	The current Debian security advisories are included on the homepage. Advisories are provided as HTML pages with links to the patches. The security advisory also contains a reference to the mailing list.
Gentoo	Info: *http://www.gentoo.org/security/en/glsa/index.xml* Forum: *http://forums.gentoo.org/* List: *http://www.gentoo.org/main/en/lists.xml* Reference: GLSA: ... 1)	The current security advisories for Gentoo are listed on the Gentoo security site linked off the homepage. Advisories are provided as HTML pages with the coding to emerge the corrected versions.
Mandrake	Info: *http://www.mandrakesecure.net* List: *http://www.mandrakesecure.net/en/mlist.php* Reference: MDKSA-... 1)	MandrakeSoft runs its own Web site on security topics. Among other things, it includes security advisories and references to the mailing lists. The advisories are HTML pages, but there are no links to the patches.
Red Hat	Info: *http://www.redhat.com/errata/* List: *http://www.redhat.com/mailing-lists/* Reference: RHSA-... 1)	Red Hat files security advisories as so-called Errata: Issues for each Red Hat Linux version are then grouped. The security advisories are provided in the form of an HTML page with links to patches.
Slackware	Info: *http://www.slackware.com/security/* List: *http://www.slackware.com/lists/* (slackware-security) Reference: [slackware-security] ... 1)	The start page contains links to the security mailing list archive. No additional information on Slackware security is available.
Suse	Info: *http://www.suse.de/uk/private/support/security/* Patches: *http://www.suse.de/uk/private/download/updates/* List: suse-security-announce Reference: SUSE-SA ... 1)	There is no longer a link to the security page after changes to the Web site. It contains information on the mailing list and the advisories. The security patches for the individual Suse Linux versions are shown in red on the general updates site. A short description of the vulnerability the patch resolves is provided

1) All distributors indicate security mails in the subject line.

Pavuk

Pavuk is an application used to mirror contents of WWW documents or files. It transfers documents from HTTP, FTP, Gopher, and optionally from HTTPS (HTTP over SSL) servers.

Ulf Härnhammar discovered a vulnerability in pavuk. In this error, an oversized HTTP 305 response sent by a malicious server could potentially cause arbitrary code to be executed with the privileges that belong to the pavuk process.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0456 to this issue. ■

Debian reference DSA-527-1 pavuk -- buffer overflow

Gentoo reference GLSA 200406-22 / Pavuk

DHCP

The Dynamic Host Configuration Protocol (DHCP) server is used to configure clients that dynamically connect to a network (WLAN hotspots, customer networks, ...).

A vulnerability in how ISC's DHCPD handles the logging code of the server with syslog messages can allow a malicious attacker with the ability to send special packets to the DHCPD listening port to crash the daemon, thus causing a Denial of Service. It is also possible that they may be able to execute arbitrary code on the vulnerable server with the permissions of the user running DHCPD, which is usually root. The United States Computer Emergency Readiness Team has assigned the name VU#317350 to this issue.

A similar vulnerability also exists in the way ISC's DHCPD makes use of the vsnprintf() function on systems that do not support vsnprintf(). This vulnerability could also be used to execute arbitrary code and/or perform a DoS attack. The vsnprintf() statements that have this problem are defined after the vulnerable code noted above, which would trigger the previous problem rather than this one. The United States Computer Emergency Readiness Team has assigned the name VU#654390 to this issue. ■

Suse reference SuSE-SA:2004:019

Mandrake reference MDKSA-2004:061

Kernel

Multiple security vulnerabilities of the Linux kernel have been found recently.

Michael Schroeder and Ruediger Oertel found that Missing Discretionary Access Control (DAC) checks in the chown(2) system call allow an attacker with a local account to change the group ownership of arbitrary files, which leads to root privileges. It is specific to version 2.6 based systems, that only local shell access is needed to exploit this vulnerability. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0497 to this issue.

A flaw was found in Linux kernel versions 2.4 and 2.6 for x86 and x86_64 that allowed local users to cause a denial of service (system crash) by triggering a signal handler with a certain sequence of fsave and frstor instructions. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0554 to this issue.

Another flaw was discovered in an error path supporting the clone() system call that allowed local users to cause a denial of service (memory leak) by passing invalid arguments to clone() running in an infinite loop of a user's program. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0427 to this issue.

Enhancements were committed to the 2.6 kernel by Al Viro which enabled the Sparse source code checking tool to check for a certain class of kernel bugs. Kernel memory access vulnerabilities are fixed in the e1000, decnet, acpi_asus, alsa, airo/WLAN, pss and mpu401 drivers. These vulnerabilities can lead to kernel memory read access, write access and local Denial of Service conditions, resulting in access to the root account for an attacker with a local account on the affected system. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0495 to these issues.

An information leak vulnerability that affects only ia64 systems was also discovered. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0565 to these issues. ■

Suse reference SUSE-SA:2004:020
Mandrake reference MDKSA-2004:066
Red Hat reference RHSA-2004:255-10

Subversion

Subversion is a version control system like the well known CVS.

The subversion code is vulnerable to a remotely exploitable buffer overflow on the heap. The error appears before any authentication takes place. An attacker is able to execute arbitrary code by abusing this vulnerability.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0413 to this issue. ■

Suse reference SuSE-SA:2004:018
Gentoo reference GLSA 200406-07 / Subversion

SquirrelMail

SquirrelMail is a webmail package written in PHP. Multiple vulnerabilities have been found which affect a version of SquirrelMail.

An SQL injection flaw was found in SquirrelMail version 1.4.2 and earlier. If SquirrelMail is configured to store user address books in the database, a remote attacker could use this flaw to execute arbitrary SQL statements. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0521 to this issue.

A number of cross-site scripting (XSS) flaws in SquirrelMail version 1.4.2 and earlier could allow remote attackers to execute script as other web users. The Common Vulnerabilities and Exposures project has assigned the names CAN-2004-0519 and CAN-2004-0520 to these issues. ■

Red Hat reference RHSA-2004:240-06
Gentoo reference GLSA 200405-16 / SquirrelMail

Libpng

An attacker could carefully craft a PNG file in such a way that it would cause an application linked to libpng to crash when opened by a victim.

A buffer overflow vulnerability was discovered in libpng due to a wrong calculation of some loop offset values. This buffer overflow can lead to Denial of Service or even remote compromise. The Common Vulnerabilities and Exposures project has assigned the name CAN-2002-1363 to this issue. ■

Mandrake reference MDKSA-2004:063
Red Hat reference RHSA-2004:249-070

Apache

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

A stack buffer overflow in mod_ssl that could be triggered if using the FakeBasicAuth option. If mod_ssl was sent a client certificate with a subject DN field longer than 6000 characters, a stack overflow occurred if FakeBasicAuth had been enabled. To exploit this issue the malicious certificate would have to be signed by a Certificate Authority which mod_ssl is configured to trust. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0488 to this issue.

A remotely triggered memory leak in the Apache HTTP Server earlier than version 2.0.50 was also discovered. This allowed a remote attacker to perform a Denial of Service attack against the server by forcing it to consume large amounts of memory. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0493 to this issue.

A Denial of Service (Dos) condition was discovered in Apache 2.x by George Guninski. This can lead to httpd consuming an arbitrary amount of memory. On 64bit systems with more than 4GB of virtual memory, this may also lead to a heap-based overflow.

A buffer overflow vulnerability was also found in Apache's mod_proxy module, which can be exploited by a remote user to potentially execute arbitrary code with the privileges of a httpd child process (user apache, by default, user www-data). This can only be exploited, however, if mod_proxy is actually in use.

Note that this bug exists in a module in the apache-common package, shared by apache, apache-ssl and apache-perl, so this update is sufficient to correct the bug for all three builds of Apache httpd. However, on systems using apache-ssl or apache-perl, httpd will not automatically be restarted. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0492 to this issue. ■

Mandrake reference MDKSA-2004:064 and MDKSA-2004:065
Red Hat reference RHSA-2004:342-10
Debian reference DSA-525-1 apache -- buffer overflow
Gentoo reference GLSA 200407-03 / Apache