Insecurity News

Neon

Multiple format string vulnerabilities were discovered in neon, an HTTP and WebDAV client library. These vulnerabilities could potentially be exploited by a malicious WebDAV server to execute arbitrary code with the privileges of the process using libneon. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0179 to this issue.

Debian reference DSA-487-1 neon -- format string

rsync

A vulnerability was discovered in rsync, a file transfer program, whereby a remote user could cause an rsync daemon to write files outside of the intended directory tree. This vulnerability is not exploitable when the daemon is configured with the 'chroot' option. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0426 to this issue.

Debian reference DSA-499-1 rsync -- directory traversal

tcpdump

tcpdump, a tool for network monitoring and data acquisition, was found to contain two vulnerabilities in versions prior to 3.81, whereby tcpdump could be caused to crash through attempts to read from invalid memory locations.

Remote attackers can cause a denial of service (DoS) via ISAKMP packets containing a Delete payload with a large number of SPI's, which causes an out-of-bounds read. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-1083 to this issue. Integer underflow in the isakmp_id_print allows remote attackers to cause a denial of service via an ISAKMP packet with an Identification payload with a length that becomes less than 8 during byte order conversion, which causes an out-of-bounds read. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0184 to this issue.

Mandrake reference MDKSA-2004:030
Debian reference DSA-478-1 tcpdump -- denial of service

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	Forum: *http://forums.gentoo.org/* List: *http://www.gentoo.org/main/en/lists.xml* Reference: GLSA: ... 1)	Unfortunately, Gentoo does not offer a website with security updates or other security information. This forum is the only alternative.
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.

XChat

XChat is an IRC client for X similar to AmIRC. A remotely exploitable vulnerability was discovered in the Socks-5 proxy code in XChat. By default, socks5 traversal is disabled, and one would also need to connect to the attacker's own custom proxy server in order for this to be exploited.

Successful exploitation could lead to arbitrary code execution as the user running XChat. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0409 to this issue.

Mandrake reference MDKSA-2004:036
Red Hat reference RHSA-2004:177
Debian reference DSA-493-1 xchat -- buffer overflow

libpng

Steve Grubb discovered an error in the Portable Network Graphics library, libpng. When processing a broken PNG image, the error handling routine will access memory that is out of bounds when creating an error message. The impact of this bug is not clear, but it could lead to a core dump in a program using libpng, or could result in a DoS (Denial of Service) condition in a daemon that uses libpng to process PNG images.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0421 to this issue.

Mandrake reference MDKSA-2004:040
Red Hat reference RHSA-2004:181
Debian reference DSA-498-1 libpng -- out of bound access

xine-ui

Shaun Colley discovered a problem in xine-ui, the xine video player user interface. A script contained in the package to possibly remedy a problem or report a bug does not create temporary files in a secure fashion.

This could allow a local attacker to overwrite arbitrary files with the privileges of the user invoking xine user interface script. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0372 to this issue.

Mandrake reference MDKSA-2004:033
Debian reference DSA-477-1 xine-ui -- insecure temporary file creation

MySQL

MySQL is a common database system. Shaun Colley discovered that two scripts distributed with MySQL, the 'mysqld_multi' and 'mysqlbug' scripts, did not create temporary files in a secure fashion. An attacker could create symbolic links in /tmp that could allow for overwriting of files with the privileges of the user running the scripts. The script mysqlbug in MySQL allows local users to overwrite arbitrary files via a symlink attack. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0381 to this issue.

The script mysqld_multi in MySQL allows local users to overwrite arbitrary files via a symlink attack. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0388 to this issue.

Mandrake reference MDKSA-2004:034
Debian reference DSA-483-1 mysql -- insecure temporary file creation

CVS

The Concurrent Versions System (CVS) offers tools which allow developers to share and maintain large software projects. Sebastian Krahmer, from the Suse security team, discovered a remotely exploitable vulnerability in the CVS client. When doing a CVS checkout or update operation over a network, the client accepts absolute pathnames in the RCS diff files. A maliciously configured server could then create any file with content on the local user's disk. This problem affects all versions of CVS prior to 1.11.15 which has fixed the problem. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0180 to this issue.

Derek Robert Price discovered another vulnerability whereby a CVS pserver could be abused by a malicious client to view the contents of certain files outside of the CVS root directory using relative pathnames containing "../". The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0405 to this issue.

Suse reference SuSE-SA:2004:008
Mandrake reference MDKSA-2004:028
Red Hat reference RHSA-2004:154
Debian reference DSA-486-1 cvs -- several vulnerabilities

Linux Kernel 2.4

A vulnerability was found in the R128 DRI driver by Alan Cox. This could theoretically allow local privilege escalation. The previous fix, only partially corrected the problem. Alan Cox and Thomas Biege have now developed a full fix for this. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0003 to this issue.

A local root vulnerability was discovered in the isofs component of the Linux 2.4 kernel code which handles ISO9660 filesystems, by iDefense. This vulnerability can be triggered by performing a directory listing on a maliciously constructed ISO filesystem, or attempting to access a file via a malformed symlink on such a filesystem. A malicious attacker exploiting this buffer overflow could gain kernel-level access to the system. Sebastian Krahmer and Ernie Petrides have developed a fix for this. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0109 to this issue.

An information leak was also discovered in the ext3 filesystem code by Solar Designer. It was discovered that when creating or writing to an ext3 filesystem, some amount of other in-memory data gets written to the device. The data is not the file's contents, not something on the same filesystem, or even anything that was previously in a file at all. To obtain this data, a user with root privileges needs to read the raw device. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0177 to this issue. The same vulnerability was also found in the XFS filesystem code (CAN-2004-0133) and the JFS filesystem code (CAN-2004-0181).

Finally, a vulnerability in the OSS code for SoundBlaster 16 devices was discovered by Andreas Kies. It is possible for local users with access to the sound system to crash the machine. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0178 to this issue.

Suse reference SuSE-SA:2004:009
Mandrake reference MDKSA-2004:029
Red Hat reference RHSA-2004:166
Debian reference DSA-495-1 linux-kernel-2.4.16 -- several vulnerabilities