Insecurity News

GnuPG

Phong Nguyen identified a severe bug in the way GnuPG creates and uses ElGamal keys for signing. This is a significant security failure which can lead to a compromise of almost all ElGamal keys used for signing. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0971 to this issue.

Debian reference DSA-429-1 gnupg – cryptographic weakness

Perl

Paul Szabo discovered a number of bugs in suidperl, a helper program to run Perl scripts with setuid privileges. By exploiting these bugs, an attacker could find information about files (such as their existence and some of their permissions) that should not be accessible to unprivileged users. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0618 to this issue.

Debian reference DSA-431-1 perl – information leak

trr19

Steve Kemp discovered a problem in trr19, a type trainer application for GNU Emacs, which is written as a pair of setgid() binaries and wrapper programs which execute commands for GNU Emacs. The binaries don't drop privileges before executing a command, allowing an attacker to gain access to the local group games. CAN-2004-0047

Debian reference DSA-430-1 trr19 – missing privilege release

Crawl

Steve Kemp from the GNU/Linux audit project discovered a problem in crawl, another console based dungeon exploration game, in the vein of nethack and rogue. The program uses several environment variables as inputs, but doesn't apply a size check before copying one of them into a fixed size buffer. CAN-2004-0103

Debian reference DSA-432-1 crawl – buffer overflow

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.

mpg123

A vulnerability was discovered in mpg123, a command-line mp3 player, whereby a response from a remote HTTP server could overflow a buffer allocated on the heap, potentially permitting execution of arbitrary code with the privileges of the user invoking mpg123.

In order for this vulnerability to be exploited, mpg321 would need to request an mp3 stream from a malicious remote server via HTTP. CAN-2003-0865

Debian reference DSA-435-1 mpg123 – heap overflow

mc

Midnight Commander (mc) is a visual shell, similar to a file manager.

A buffer overflow has been found in Midnight Commander's virtual filesystem code. This is a stack-based buffer overflow in vfs_s_resolve_symlink of vfs/direntry.c that allows remote attackers to execute arbitrary code during symlink conversion. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-1023 to this issue.

Mandrake reference MDKSA-2004:007
Red Hat reference RHSA-2004:034-03
Debian reference DSA-424-1 mc – buffer overflow

Slocate

Slocate is a security-enhanced version of locate, designed to index and find files on a system via a central database.

Patrik Hornik discovered a vulnerability in Slocate versions up to and including 2.7 whereby a specially crafted database could overflow a heap-based buffer. This vulnerability could be exploited by a local attacker to gain the privileges of the "slocate" group, which can access the global database containing a list of pathnames of all files on the system, including those which should only be visible to privileged users.

This problem, and a category of potentially similar problems, have been fixed by modifying slocate to drop privileges before reading a user-supplied database. CAN-2003-0848

Mandrake reference MDKSA-2004:004
Red Hat reference RHSA-2004:040-02
Debian reference DSA-428-1 slocate – buffer overflow

Kdepim

A vulnerability has been discovered in all versions of kdepim as distributed with KDE versions 3.1.0 through 3.1.4. This vulnerability allows for a carefully crafted .VCF file to potentially enable a local attacker to compromise the privacy of a victim's data or execute arbitrary commands with the victim's privileges.

This can also be used by remote attackers if the victim enables previews for remote files; fortunately, this option is disabled by default. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0988 to this issue.

Mandrake reference MDKSA-2004:003

NetPBM

The netpbm package contains a library of functions that support programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps), and others.

A number of temporary file bugs have been found in versions of NetPBM. Many of these programs were found to create temporary files in an insecure manner, which could allow a local attacker to overwrite files with the privileges of the user invoking a vulnerable netpbm tool. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0924 to this issue.

Red Hat reference RHSA-2004:030-01
Debian reference DSA-426-1 netpbm-free – insecure temporary files

Mailman

Mailman is a mailing list manager.

Dirk Mueller discovered a cross-site scripting bug in the admin interface in versions of Mailman 2.1 before 2.1.4. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0965 to this issue.

A cross-site scripting bug in the 'create' CGI script affects versions of Mailman 2.1 before 2.1.3. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0992 to this issue.

CAN-2003-0038 potential cross-site scripting via certain CGI parameters (not known to be exploitable in this version)

CAN-2003-0991 certain malformed email commands could cause the mailman process to crash. The cross-site scripting vulnerabilities could allow an attacker to perform administrative operations without authorization, by stealing a session cookie.

Red Hat reference RHSA-2004:020-02
Debian reference DSA-436-1 mailman – several vulnerabilities

Gaim

Gaim is an instant messenger client that can handle multiple protocols. A number of vulnerabilities were discovered in Gaim by Stefan Esser, while auditing the Gaim source code, versions 0.75 and earlier. These can lead to a remote system compromise with the privileges of the user running GAIM. Thanks to Jacques A. Vidrine for providing initial patches.

Due to the nature of instant messaging many of these bugs require man-in-the-middle attacks between client and server. However at least one of the buffer overflows could be exploited by an attacker sending a carefully-constructed malicious message through a server.

CAN-2004-0005 When the Yahoo Messenger handler decodes an octal value for email notification functions, two different kinds of overflows can be triggered. When the MIME decoder decodes a quoted printable encoded string for email notification, two other different kinds of overflows can be triggered. These problems only affect the version in the unstable distribution.

CAN-2004-0006 When parsing the cookies within the HTTP reply header of a Yahoo web connection, a buffer overflow can happen. When parsing the Yahoo Login Webpage, the YMSG protocol overflows stack buffers if the web page returns oversized values. When splitting an URL into its parts, a stack overflow can be caused. These problems only affect the version in the unstable distribution.

When an oversized keyname is read from a Yahoo Messenger packet, a stack overflow can be triggered. When Gaim is set up to use a HTTP proxy for connecting to the server, a malicious HTTP proxy can exploit it. These problems affect all versions Debian ships.

However, the connection to Yahoo doesn't work in the version in Debian stable.

CAN-2004-0007 Internally data is copied between two tokens into a fixed size stack buffer without a size check. This only affects the version of Gaim in the unstable distribution.

CAN-2004-0008 When allocating memory for AIM/Oscar DirectIM packets an integer overflow can happen, resulting in a heap overflow. This only affects the version of Gaim in the unstable distribution.

Suse reference SuSE-SA:2004:004
Mandrake reference MDKSA-2004:006-1
Red Hat reference RHSA-2004:032-04
Debian reference DSA-434-1 gaim – several vulnerabilities

Tcpdump

Tcpdump is a well known command line tool for administrators to monitor and analyze network traffic. A number of vulnerabilities were discovered by George Bakos in tcpdump versions prior to 3.8.1 that, if fed a maliciously crafted packet, could be exploited to crash tcpdump or potentially execute arbitrary code with the privileges of the user running tcpdump.

Jonathan Heusser discovered an additional flaw in the ISAKMP decoding routines for tcpdump 3.8.1 and earlier. Jonathan also found a flaw in the print_attr_string function in the RADIUS decoding routines for tcpdump 3.8.1 and earlier. These vulnerabilities include:

An infinite loop and memory consumption processing L2TP packets (CAN-2003-1029). A segmentation fault caused by a RADIUS attribute with a large length value (CAN-2004-0055). Infinite loops in processing ISAKMP packets (CAN-2003-0989, CAN-2004-0057).

Remote attackers could potentially exploit these issues by sending carefully-crafted packets to a victim. If the victim uses tcpdump, these packets could result in a denial of service, or possibly execute arbitrary code as the 'pcap' user.

Suse reference SuSE-SA:2004:002
Mandrake reference MDKSA-2004:008
Red Hat reference RHSA-2004:007-10
Debian reference DSA-425-1 tcpdump – multiple vulnerabilities