Insecurity News

XaoS

XaoS, a program for displaying fractal images, is installed setuid root on certain architectures in order to use svgalib, which requires access to the system video hardware. It is not designed for secure setuid execution, and can be exploited to gain root privileges.

New updated packages are available in which the setuid bit has been removed. Users who require the svgalib functionality should grant these privileges only to a trusted group.

Debian reference DSA-310-1 xaos – improper setuid-root execution

Fuzz

Joey Hess discovered that fuzz, a software stress-testing tool, creates a temporary file without taking appropriate security precautions. This bug could allow an attacker to gain the privileges of the user invoking fuzz, excluding root (fuzz does not allow itself to be invoked as root).

Debian reference DSA-302-1 fuzz – privilege escalation

Gzip

Paul Szabo discovered that znew, a script included in the gzip package, creates its temporary files without taking precautions to avoid a symlink attack. This could allow local users to overwrite arbitrary files via a symlink attack on temporary files.

The gzexe script has a similar vulnerability which was patched in an earlier release, but inadvertently reverted.

Debian reference DSA-308-1 gzip – insecure temporary files

Leksbot

Maurice Massar has discovered that, due to a packaging error, the program /usr/bin/KATAXWR was inadvertently installed setuid root. As this program was not designed to run as setuid and contained multiple vulnerabilities which could be exploited to gain root privileges it should be upgraded as soon as possible to safe guard security.

Debian reference DSA-299-1 leksbot – improper setuid-root execution

Security Posture of Major Distributions

Distributor	Security Sources	Comment
Debian	Info: *www.debian.org/security/*, List: debian-security-announce, Reference: DSA-... [1]	Debian have integrated current security advisories on their web site. The advisories take the form of HTML pages with links to patches. The security page also contains a note on the mailing list.
Mandrake	Info: *www.mandrakesecure.net*, List: security-announce, Reference: MDKSA-... [1]	MandrakeSoft run a web site dedicated to security topics. Amongst other things the site contains security advisories and references to mailing lists. The advisories are HTML pages, but there are no links to the patches.
Red Hat	Info: *www.redhat.com/errata/* List: *www.redhat.com/mailing-lists/* (linux-security and redhat-announce-list) Reference: RHSA-... [1]	Red Hat categorizes security advisories as Errata: Under the Errata headline any and all issues for individual Red Hat Linux versions are grouped and discussed. The security advisories take the form of HTML pages with links to patches.
SCO	Info: *www.sco.com/support/security/*, List: *www.sco.com/support/forums/announce.html*, Reference: CSSA-... [1]	You can access the SCO security page via the support area. The advisories are provided in clear text format.
Slackware	List: *www.slackware.com/lists/* (slackware-security), Reference: slackware-security ... [1]	Slackware do not have their own security page, but do offer an archive of the Security mailing List.
SuSE	Info: *www.suse.de/uk/private/support/security/*, Patches: *www.suse.de/uk/private/download/updates/*, List: suse-security-announce, Reference: suse-security-announce ... [1]	There is a link to the security page on the homepage. The security page contains information on the mailing list and advisories in text format. Security patches for individual SuSE Linux versions are marked red on the general update page and comprise a short description of the patched vulnerability.

[1] Security mails are available from all the above-mentioned distributions via the reference provided.

GPS

GPS is a graphical application to watch system processes. In the new release 1.1.0 of the gps package, several security vulnerabilities were fixed. These include a bug fix on rgpsp connection source acceptation policy (any host can connect even when the config file told otherwise).

Thanks to Stanislav Ievlev from ALT-Linux, several possibilities of buffer overflows have been fixed.

- fixed the misformatting of command line parameters in rgpsp protocol
- fixed buffer overflow error that caused rgpsp to SIGSEGV when stating processes with large command lines (> 128 chars)

All of these problems affect Debian's gps package version 0.9.4-1 in the Debian Woody distribution.

Debian reference DSA-307-1 gps – multiple

Sendmail

Paul Szabo discovered bugs in three scripts included within the sendmail package. With these scripts, temporary files were created insecurely (expn, checksendmail and doublebounce.pl). These errors could allow an attacker to gain the privileges of a user, including root, when invoking the script .

Debian reference DSA-305-1 sendmail – insecure temporary files

MySQL

With the combination of two errors, there is a risk of privilege escalation.

CAN-2003-0073: The MySQL package contains a bug whereby dynamically allocated memory is freed more than once, which could be deliberately triggered by an attacker to cause a crash, resulting in a denial of service condition. In order to exploit this vulnerability, a valid username and password for access to the MySQL server is required.

CAN-2003-0150: The MySQL package contains a bug whereby a malicious user, granted certain permissions within MySQL, could create a configuration file which would cause the MySQL server to run as root, or any other user, rather than the MySQL user.

Debian reference DSA-303-1 mysql – privilege escalation

Lv

Leonard Stiles discovered that lv, a multilingual file viewer, would read options from a configuration file in the current directory. Because such a file could be placed there by a malicious user, and lv configuration options can be used to execute commands, this represented a security vulnerability. An attacker could gain the privileges of the user invoking lv, including root.

Debian reference DSA-304-1 lv – privilege escalation

Ghostscript

A vulnerability was discovered in Ghostscript versions prior to 7.07 that allowed malicious postscript files to execute arbitrary commands even when -dSAFER is enabled.

Mandrake reference MDKSA-2003:065 : ghostscript

Apache 2

Two vulnerabilities were discovered in the Apache web server that affect all 2.x versions prior to 2.0.46. The first, discovered by John Hughes, is a build system problem that allows remote attackers to prevent access to authenticated content when a threaded server is used. This only affects versions of Apache compiled with threaded server "httpd.worker".

The second vulnerability, discovered by iDefense, allows remote attackers to cause a DoS (Denial of Service) condition and may also allow the execution of arbitrary code.

Mandrake reference MDKSA-2003:063-1 : apache2

Kopete

A vulnerability was discovered in versions of kopete, a KDE instant messenger client, prior to 0.6.2. This vulnerability is in the GnuPG plugin that allows for users to send each other GPG-encrypted instant messages. The plugin passes encrypted messages to gpg, but does no checking to sanitize the commandline before it is passed to gpg. This can allow remote users to execute arbitrary code, with the permissions of the user running kopete, on the local system.

Mandrake reference MDKSA-2003:055 : kopete

GnuPG

A bug was discovered in GnuPG versions 1.2.1 and earlier. This occurs when gpg evaluates trust values for different UIDs assigned to a key. It would incorrectly associate the trust value of the UID with the highest trust value with every other UID assigned to that key. This prevents a warning message from being given when attempting to encrypt to an invalid UID, but due to the bug, is accepted as valid.

Mandrake reference MDKSA-2003:061 : gnupg

Cdrecord

A vulnerability in cdrecord was discovered that can be used to obtain root access because Mandrake Linux ships with the cdrecord binary suid root and sgid cdwriter.

You can remove the suid and sgid bits from cdrecord manually, which can be done by executing, as root:

```
chmod ug-s /usr/bin/cdrecord
```

Mandrake reference MDKSA-2003:058-1 : cdrecord

Xinetd

A vulnerability was discovered in xinetd where memory was allocated and never freed if a connection was refused for any reason. Because of this bug, an attacker could crash the xinetd server, making unavailable all of the services it controls. Other flaws were also discovered that could cause incorrect operation in certain strange configurations.

Mandrake reference MDKSA-2003:056 : xinetd

Man

A difficult to exploit vulnerability was discovered in versions of man prior to 1.5l. A bug exists in man that could cause a program named "unsafe" to be executed due to a malformed man file. In order to exploit this bug, a local attacker would have to be able to get another user to read the malformed man file, and the attacker would also have to create a file called "unsafe" that would be located somewhere in the victim's path.

Mandrake reference MDKSA-2003:054 : man

Snort

An integer overflow was discovered in the Snort stream4 pre-processor by the Sourcefire Vulnerability Research Team. This preprocessor (spp_stream4) incorrectly calculates segment size parameters during stream reassembly for certain sequence number ranges. This can lead to an integer overflow that can in turn lead to a heap overflow that can be exploited to perform a denial of service (DoS) or even remote command excution on the host running Snort.

Disabling the stream4 pre-processor will make Snort invulnerable to this attack, and the flaw has been fixed upstream in Snort version 2.0. Snort versions 1.8 through 1.9.1 are vulnerable.

Mandrake reference MDKSA-2003:052 : snort

Tcpdump

Tcpdump is a command-line tool for monitoring network traffic.

The Red Hat tcpdump packages advertise that by default tcpdump will drop permissions to user 'pcap'. Due to a compilation error this did not happen, and tcpdump would run as root unless the '-U' flag was specified. Users of tcpdump are advised to upgrade to these errata packages, which contain are compiled so that by default tcpdump will drop privileges to the 'pcap' user.

Red Hat reference RHSA-2003:174-04

CUPS

CUPS is used as the default print spooler on new installations of Red Hat Linux 9, and has been provided (but not as the default) for Red Hat Linux 7.3 and 8.0.

Phil D'Amore of Red Hat discovered a vulnerability in the CUPS IPP (Internet Printing Protocol) implementation. The IPP implementation is single-threaded, which means only one request can be serviced at a time. An attacker could make a partial request that does not time out and therefore creates a denial of service. In order to exploit this bug, an attacker must have the ability to make a TCP connection to the IPP port (by default 631). This vulnerability has been fixed upstream in CUPS 1.1.19 and packages of previous versions have been fixed to correct the problem.

Red Hat reference RHSA-2003:171-14