Insecurity News

Teapop

Teapop, a POP-3 server, includes modules for authenticating users against a PostgreSQL or MySQL database. These modules do not properly escape user-supplied strings before using them in SQL queries. This vulnerability could be exploited to execute arbitrary SQL code under the privileges of the database user as which Teapop has authenticated. ■

Debian reference DSA-347-1 Teapop – SQL injection

skk, ddskk

skk (Simple Kana to Kanji conversion program), does not take appropriate security precautions when creating temporary files. This bug could potentially be exploited to overwrite arbitrary files with the privileges of the user running Emacs and skk.

ddskk is derived from the same code, and contains the same bug. ■

Debian reference DSA-343-1 skk, ddskk – insecure temporary file

ECLiPt Roaster

ECLiPt Roaster, which is a front-end for burning CD-R media using cdrecord, does not take appropriate security precautions when creating a temporary file for use as a lockfile. This bug could potentially be exploited to overwrite arbitrary files with the privileges of the user running ECLiPt Roaster and thus lead to potential vulnerabilities within a system. A new updated package is now available. ■

Debian reference DSA-366-1 ERoaster – insecure temporary file

fdclone

fdclone creates a temporary directory in /tmp as a workspace. However, if this directory already exists, the existing directory is used instead, regardless of its ownership or permissions. This would allow an attacker to gain access to fdclone's temporary files and their contents, or replace them with other files under the attacker's control. ■

Debian reference DSA-352-1 fdclone – insecure temporary directory

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.

unzip

A directory traversal vulnerability in UnZip 5.50 allows attackers to bypass a check for relative pathnames ("../") by placing certain invalid characters between the two "." characters. ■

Debian reference DSA-344-1 unzip – directory traversal

wu-ftpd

iSEC Security Research reports that wu-ftpd contains an off-by-one bug in the fb_realpath function which could be exploited by a logged-in user (local or anonymous) to gain root privileges. A demonstration exploit is reportedly available. ■

Debian reference DSA-357-1 wu-ftpd – remote root exploit

man-db

man-db provides the standard man(1) command on Debian systems. During configuration of this package, the administrator is asked whether man(1) should run setuid to a dedicated user ("man") in order to provide a shared cache of preformatted manual pages. The default is for man(1) NOT to be setuid, and in this configuration no known vulnerability exists. However, if the user explicitly requests setuid operation, a local attacker could exploit either of the following bugs to execute arbitrary code as the "man" user.

Again, these vulnerabilities do not affect the default configuration, where man is not setuid.

Multiple buffer overflows in man-db 2.4.1 and earlier, when installed setuid, allow local users to gain privileges via (1) MANDATORY_MANPATH, MANPATH_MAP, and MANDB_MAP arguments to add_to_dirlist in manp.c, (2) a long pathname to ult_src in ult_src.c, (3) a long .so argument to test_for_include in ult_src.c, (4) a long MANPATH environment variable, or (5) a long PATH environment variable.

Certain DEFINE directives in ~/.manpath, which contained commands to be executed, would be honored even when running setuid, allowing any user to execute commands as the "man" user. ■

Debian reference DSA-364-1 man-db – buffer overflows, arbitrary command execution

gallery

Larry Nguyen discovered a cross site scripting vulnerability in gallery, a web-based photo album written in php. This security flaw can allow a malicious user to craft a URL that executes Javascript code on your website.

Debian reference DSA-355-1 gallery – cross-site scripting

xbl

Another buffer overflow was discovered in xbl, distinct from the one addressed in DSA-327 (CAN-2003-0451), involving the -display command line option. This vulnerability could be exploited by a local attacker to gain gid 'games'.

Debian reference DSA-345-1 xbl – buffer overflow

phpGroupWare

Multiple cross-site scripting (XSS) vulnerabilities in phpGroupWare 0.9. 14.003 (aka webdistro) allow remote attackers to insert arbitrary HTML or web script, as demonstrated with a request to index.php in the addressbook module.

Unknown vulnerability in the Virtual File System (VFS) capability for phpGroupWare 0.9.16preRC and versions before 0.9.14.004 with unknown implications, related to the VFS path being under the web document root.

Multiple SQL injection vulnerabilities in the infolog module of phpGroupWare could allow remote attackers to execute arbitrary SQL statements.

Debian reference DSA-365-1 phpGroupWare – several vulnerabilities

OpenSSH

A vulnerability has been found that can result in an information leak caused by sshd's interaction with the PAM system. OpenSSH is a suite of network connectivity tools that can be used to establish encrypted connections between systems on a network and can provide interactive login sessions and port forwarding, among other functions.

When configured to allow password based or challenge-response authentication, sshd (the OpenSSH server) uses PAM (Pluggable Authentication Modules) to verify the user's password. Under certain conditions, OpenSSH versions prior to 3.6.1p1 reject an invalid authentication attempt without first attempting any authentication using PAM.

If PAM is configured with its default failure delay, the amount of time sshd takes to reject an invalid authentication request varies widely enough that the timing variations could be used to deduce whether or not an account with a specified name existed on the server. This information could then be used to narrow the focus of an attack against some other system component.

Red Hat reference RHSA-2003:222-08

GtkHTML

GtkHTML is the HTML rendering widget used by the Evolution mail reader.

GtkHTML supplied with versions of Evolution prior to 1.2.4 contains a bug when handling HTML messages. Alan Cox discovered that certain malformed messages could cause the Evolution mail component to crash.

Red Hat reference RHSA-2003:126-06

nfs-utils

The nfs-utils package provides a daemon for the kernel NFS server and some related tools.

Janusz Niewiadomski has found a buffer overflow error in nfs-utils version 1.0.3 and earlier. This bug could be exploited by an attacker, causing a remote Denial of Service (crash). It is not believed that this bug could lead to remote arbitrary code execution.

Red Hat reference RHSA-2003:206-08

postfix

Postfix is a Mail Transport Agent (MTA).

Two security issues have been found in recently supplied versions of Postfix.

Postfix versions before 1.1.12 allow an attacker to bounce-scan private networks, or use the daemon as a DDoS tool by forcing the daemon to connect to an arbitrary service at an arbitrary IP address and receiving either a bounce message or observing queue operations to infer the status of the delivery attempt.

Postfix versions from 1.1 up to and including 1.1.12 have a bug where a remote attacker could send a malformed envelope address to cause the queue manager to lock up until an entry is removed from the queue, or lock up the SMTP listener, leading to a DoS.

Red Hat thank Michal Zalewski for discovering and disclosing the flaws and to Wietse Venema for providing patches.

Red Hat reference RHSA-2003:251-07

MS for UNIX Telnet server

The telnet server included in the Microsoft Services for Unix (SFU) package contains a memory leak that can lead to excessive resource consumption on affected systems.

This vulnerability affects Microsoft Windows NT 4.0 and Windows 2000 systems that have the SFU package installed. It does not affect the telnet server that ships with Windows NT 4.0 and Windows 2000.

CERT reference Vulnerability Note VU#994851

EnGarde

Stunnel is an SSL wrapper used in EnGarde to tunnel SIMAP and SPOP3. A potential vulnerability has been found when stunnel is configured to listen to incoming connections for these services.

Guardian Digital Security Advisory reference ESA-20030806-020

mpg123

A vulnerability in the mpg123 mp3 player could allow local and/or remote attackers to cause a DoS and possibly execute arbitrary code via an mp3 file with a zero bitrate, which causes a negative frame size.

Mandrake reference MDKSA-2003:078

GnuPG

GnuPG needs to be setuid to make use of protected memory space, however the setgid bit allowed a gpg user to overwrite group root writable files and is therefore unnecessary.

It is recommended that all Gentoo Linux users who are running app-crypt/gnupg upgrade to gnupg-1.2.2-r1 as follows

```
emerge sync
emerge gnupg
emerge clean
```

GENTOO reference 200307-06