Insecurity News

mozart

mozart, a development platform based on the Oz language, includes MIME configuration data which specifies that Oz applications should be passed to the Oz interpreter for execution.

This means that file managers, web browsers, and other programs which honor the mailcap file could automatically execute Oz programs downloaded from untrusted sources. Thus, a malicious Oz program could execute arbitrary code under the uid of a user running a MIME-aware client program if the user selected a file (for example, choosing a link in a web browser).

Debian reference DSA-342-1 mozart – unsafe mailcap configuration

cupsys

The CUPS print server in Debian is vulnerable to a denial of service when an HTTP request is received without being properly terminated.

Debian reference DSA-317-1 cupsys – denial of service

liece

liece, an IRC client for Emacs, does not take the appropriate security precautions when it is creating temporary files. This vulnerability could potentially be exploited to overwrite arbitrary files with the same privileges of the user who is running Emacs and *liece*, theoretically with the contents supplied by the attacker.

Debian reference DSA-341-1 liece – insecure temporary file

ProFTPd

runlevel@raregazz.org has reported that ProFTPd's PostgreSQL authentication module is vulnerable to a SQL injection attack. This vulnerability could be exploited by a remote, unauthenticated attacker to execute arbitrary SQL statements, potentially exposing the passwords of other users, or to connect to ProFTPd as an arbitrary user without supplying the correct password.

Debian reference DSA-338-1 proftpd – SQL injection

mantis

mantis, a PHP/MySQL web based bug tracking system, stores the password used to access its database in a configuration file which is world-readable. This could allow a local attacker to read the password and gain read/write access to the database.

Debian reference DSA-335-1 mantis – incorrect permissions

tcptraceroute

tcptraceroute is a setuid-root program which drops root privileges after obtaining a file descriptor used for raw packet capture. However, it did not fully relinquish all privileges, and in the event of an exploitable vulnerability, root privileges could be regained.

No current exploit is known, but this safeguard is being repaired in order to provide a measure of containment in the event that a flaw should be discovered.

Debian reference DSA-330-1 tcptraceroute – failure to drop root privileges

lyskom-server

Calle Dybedahl found a bug in *lyskom-server* which could result in a denial of service where an unauthenticated user could cause the server to become unresponsive as it processes a large query.

Debian reference DSA-318-1 lyskom-server – denial of service

webmin

miniserv.pl in the webmin package does not properly handle metacharacters, such as line feeds and carriage returns, in Base64-encoded strings used in Basic authentication. This vulnerability allows remote attackers to spoof a session ID, and thereby gain root privileges.

Debian reference DSA-319-1 webmin – session ID spoofing

noweb

Jakob Lell discovered a bug in the *noroff* script included in Noweb whereby a temporary file was created insecurely. During a review, several other instances of this problem were found and fixed. These bugs could be exploited by a local user to overwrite arbitrary files owned by the user.

Debian reference DSA-323-1 noweb – insecure temporary files

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.

acm

acm, a multi-player aerial combat simulation, uses a network protocol based on the same RPC implementation used in many C libraries.

This implementation was found to contain an integer overflow vulnerability which could be exploited to execute arbitrary code.

Debian reference DSA-333-1 acm – integer overflow

webfs

webfs, a lightweight HTTP server for static content, contains a buffer overflow whereby a long Request-URI in an HTTP request could cause arbitrary code to be executed.

Debian reference DSA-328-1 webfs – buffer overflow

semi

semi, a MIME library for GNU Emacs, 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 *semi*, potentially with contents supplied by the attacker.

wemi is a fork of semi, and contains the same bug.

Debian reference DSA-339-1 semi – insecure temporary file

unzip

A vulnerability was discovered in *unzip* 5.50 and earlier that allows attackers to overwrite arbitrary files during archive extraction by placing non-printable characters between two "." characters. These invalid characters are filtered which results in a ".." sequence.

Mandrake reference MDKSA-2003:073 : unzip

xpdf

Martyn Gilmore has discovered some flaws in various PDF viewers, including *xpdf*. An attacker could place malicious external hyperlinks into a document that, if followed, could execute arbitrary shell commands with the privileges of the person who is viewing the PDF document.

Mandrake reference MDKSA-2003:071 : xpdf

ethereal

A number of string handling bugs were found within the packet dissectors in the *ethereal* program that can be exploited using specially crafted packets to cause ethereal to consume excessive amounts of memory, crash, or even execute arbitray code.

These vulnerabilities have now been fixed upsteam in the ethereal version 0.9.13.

Mandrake reference MDKSA-2003:070 : ethereal

BitchX

A Denial Of Service (DoS) vulnerability was discovered in the BitchX package that would allow a remote attacker to crash BitchX by changing certain channel modes. This vulnerability has been fixed in CVS and patches are now available.

Mandrake reference MDKSA-2003:069 : BitchX

gzip

A vulnerability exists in *znew*, a script included with *gzip*, that would create temporary files without taking precautions to avoid a symlink attack. Patches have been applied to make use of *mktemp* to generate unique filenames, and properly make use of *noclobber* in the script.

Likewise, a fix for *gzexe* which had been applied previously was incomplete. It has been fixed to make full use of mktemp everywhere a temporary file is created.

The *znew* problem was initially reported by Michal Zalewski and was again reported more recently to Debian by Paul Szabo.

Mandrake reference MDKSA-2003:068 : gzip

radiusd-cistron

The package *radiusd-cistron* is an implementation of the RADIUS protocol. Unfortunately the RADIUS server handles too large NAS numbers incorrectly.

This leads to the overwriting of internal memory of the server process and may be abused to gain remote access to the system the RADIUS server is running on.

SuSE reference SuSE-SA:2003:030

PHP

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP server.

A number of bugs discovered include the use of a PHP script as an ErrorDocument and possible POST body corruption in some configurations.

In PHP version 4.3.1 and earlier, when transparent session ID support is enabled using the *session.use_trans_sid* option, the session ID is not escaped before use. This allows a Cross Site Scripting attack.

Red Hat reference RHSA-2003:204-11

ypserv

The *ypserv* package contains the Network Information Service (NIS) server.

A vulnerability has been discovered in the *ypserv* NIS server prior to version 2.7. If a malicious client queries ypserv via TCP and subsequently ignores the server's response, *ypserv* will block attempting to send the reply. This results in *ypserv* failing to respond to other client requests.

Versions 2.7 and above of *ypserv* have been altered to fork a child for each client request, thus preventing any one request from causing the server to block.

Red Hat reference RHSA-2003:173-07

kon2

Janusz Niewiadomski found a vulnerability in *kon2* which allows local users to obtain root privileges.

KON is a Kanji emulator for the console. There is a buffer overflow vulnerability in the command line parsing code portion of the *kon* program up to and including version 0.3.9b. This vulnerability, if appropriately exploited, can lead to local users being able to gain elevated (root) privileges.

Red Hat reference RHSA-2003:047-15

nfs-utils

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

Red Hat reference RHSA-2003:206-05