Insecurity News

w3m

Hironori Sakamoto, one of the w3m developers, found two security vulnerabilities in w3m and associated programs. The w3m browser does not properly escape HTML tags in relation to frame contents and img alt attributes. A malicious HTML frame or img alt attribute may deceive a user to send his local cookies which are used for configuration. The information is not leaked automatically, though.

For the stable distribution (woody) these problems have been fixed in version 0.3-2.4. ■

Debian reference DSA-251-1 w3m – missing HTML quoting

mhc

It has been discovered that adb2mhc from the mhc-utils package. The default temporary directory uses a predictable name. This adds a vulnerability that allows a local attacker to overwrite arbitrary files the users has write permissions for. ■

Debian reference DSA-256-1 mhc – insecure temporary file

tcpdump

Andrew Griffiths and iDEFENSE Labs discovered a problem in tcpdump, a powerful tool for network monitoring and data acquisition. An attacker is able to send a specially crafted network packet which causes tcpdump to enter an infinite loop.

In addition to the above problem the tcpdump developers discovered a potential infinite loop when parsing malformed BGP packets. They also discovered a buffer overflow that can be exploited with certain malformed NFS packets. ■

Debian reference DSA-255-1 tcpdump – infinite loop

Sendmail

Mark Dowd of ISS X-Force found a bug in the header parsing routines of sendmail: it could cause a buffer overflow when encountering addresses with very long comments. Since sendmail also parses headers when forwarding emails this vulnerability can hit mail-servers which do not deliver the email as well.

This has been fixed in upstream release 8.12.8, version 8.12.3-5 of the package for Debian GNU/Linux 3.0/woody and version 8.9.3-25 of the package for Debian GNU/Linux 2.2/potato. ■

Debian reference DSA-257-1 sendmail – remote exploit

openssl

A vulnerability has been discovered in OpenSSL, a Secure Socket Layer (SSL) implementation. In an upcoming paper, Brice Canvel (EPFL), Alain Hiltgen (UBS), Serge Vaudenay (EPFL), and Martin Vuagnoux (EPFL, Ilion) describe and demonstrate a timing-based attack on CBC cipher suites used in SSL and TLS. OpenSSL has been found to be vulnerable to this attack. ■

Debian reference DSA-253-1 openssl – information leak

IM

Internet Message (IM) is a series of user interface commands and backend Perl5 libraries that integrate email and the NetNews user interface. They are designed to be used from both the Mew mail reader for Emacs and the command line.

A vulnerability has been discovered by Tatsuya Kinoshita in the way two IM utilities create temporary files. By anticipating the names used to create files and directories stored in /tmp, it may be possible for a local attacker to corrupt or modify data as another user. ■

Red Hat reference RHSA-2003:039-06

SquirrelMail

Two vulnerabilities have been found that affect versions of SquirrelMail shipped with Red Hat Linux 8.0.

A cross-site scripting (XSS) vulnerability in Squirrelmail version 1.2.10 and earlier allows remote attackers to execute script as other web users via read_body.php. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2002-1341 to this issue.

An incomplete fix for a cross-site scripting vulnerability in SquirrelMail 1.2.8 calls the strip_tags function on the PHP_SELF value but does not save the result back to that variable, leaving it open to cross-site scripting attacks. (CAN-2002-1276) ■

Red Hat reference RHSA-2003:042-07

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.

VTE

VTE is an terminal emulator widget used by software such as gnome-terminal.

One feature that most terminal emulators support is the ability for the shell to set the title of the window using an escape sequence.

Certain xterm variants also provide an escape sequence for reporting the current window title. This essentially takes the current title and places it directly on the command line. This feature could be potentially exploited if an attacker can cause carefully crafted escape sequences to be displayed on a vulnerable terminal emulator used by their victim.

Since it is not possible to embed a carriage return into the window title itself, the attacker would have to convince the victim to hit enter for it to process the title as a command, although the attacker can perform a number of actions to increase the likelyhood of this happening.

VTE is vulnerable to this issue and is used as the default terminal emulator for versions of gnome-terminal shipped with Red Hat Linux 8.0. Previous releases of Red Hat Linux do not contain a vulnerable version of gnome-terminal.

Red Hat reference RHSA-2003:053-10

cvs

CVS (Concurrent Versions System) is a version control system which helps to manage concurrent editing of files by various authors.

Stefan Esser of e-matters reported a "double free" bug in CVS server code for handling directory requests. This free() call allows an attacker with CVS read access to compromise a CVS server.

Additionally two features ('Update-prog' and 'Checkin-prog') were disabled to stop clients with write access to execute arbitrary code on the server. These features may be configurable at run-time in future releases of CVS server.

There is no temporary fix known other then to disable public access to the CVS server. You do not need to update the cvs package as long as you need - 'Update-prog' and 'Checkin-prog' feature and work in a trusted environment.

SuSE reference SuSE-SA:2003:0007

libmcrypt

Libmcrypt is a data encryption library that is able to load crypto-modules at run-time by using libltdl.

Versions of libmcrypt prior to 2.5.5 include several buffer overflows that can be triggered by passing very long input to the mcrypt_* functions. The way libmcrypt handles dynamic crypto-modules via libltdl leads to memory-leaks that can cause a Denial-of-Service condition. This Problem can just be solved by linking modules static. This security update does not solve the memory-leak problem to avoid compatibility problems.

Future releases of libmcrypt will be linked statically. To add the new library to the shared library cache you have to run ldconfig(8) as root. Additionally every program that is linked with libmcrypt needs to be restarted. ldd(1) can be used to find out which libraries are used by a program. Another way to determine which process uses a shared library that had been deleted is:

```
lsof -n 2>/dev/null | grep ➥
RPMDELETE | cut -d " " -f 1 | ➥
sort | uniq
```

There is no temporary fix known.

SuSE reference SuSE-SA:2003:0010

vnc

A vulnerability was discovered in the VNC server script that generates an X cookie, used by X authentication.

The script generated a cookie that was not strong enough and could allow an attacker to more easily guess the authentication cookie, thus obtaining unauthorized access to the VNC server.

Mandrake reference MDKSA-2003:022

krb5

A vulnerability was discovered in the Kerberos FTP client.

When the client retrieves a file that has a filename beginning with a pipe character, the FTP client will pass that filename to the command shell in a system() call. This could allow a malicious remote FTP server to write to files outside of the current directory or even execute arbitrary commands as the user using the FTP client.

Mandrake reference MDKSA-2003:021

shadow-utils

The shadow-utils package contains the tool useradd, which is used to create or update new user information.

When useradd creates an account, it would create it with improper permissions; instead of having it owned by the group mail, it would be owned by the user's primary group. If this is a shared group (ie. "users"), then all members of the shared group would be able to obtain access to the mail spools of other members of the same group. A patch to useradd has been applied to correct this problem.

Mandrake reference MDKSA-2003:026

Webmin

A vulnerability was discovered in webmin by Cintia M. Imanishi, in the miniserv.pl program, which is the core server of webmin. This vulnerability allows an attacker to spoof a session ID by including special metacharacters in the BASE64 encoding string used during the authentication process. This could allow an attacker to gain full administrative access to webmin.

Mandrake reference MDKSA-2003:025

lynx

A vulnerability was discovered in lynx, a text-mode web browser.

The HTTP queries that lynx constructs are from arguments on the command line or the $WWW_HOME environment variable, but lynx does not properly sanitize special characters such as carriage returns or linefeeds. Extra headers can be inserted into the request because of this, which can cause scripts that use lynx to fetch data from the wrong site from servers that use virtual hosting.

Mandrake reference MDKSA-2003:023

pam

Andreas Beck discovered that the pam_xauth module would forward authorization information from the root account to unprivileged users. This can be exploited by a local attacker to gain access to the root user's X session. In order for it to be successfully exploited, the attacker would have to somehow get the root user to su to the account belonging to the attacker.

Mandrake reference MDKSA-2003:017