Insecurity News

Node

Morgan, alias SM6TKY, discovered and fixed several security related problems in LinuxNode, an Amateur Packet Radio Node program. The buffer overflow he discovered can be used to gain unauthorised root access and can be remotely triggered.

Debian reference DSA-375-1 node – buffer overflow, format string

Netris

Shaun Colley discovered a buffer overflow vulnerability in netris, a network version of a popular puzzle game. A netris client connecting to an untrusted netris server could be sent an unusually long data packet, which would be copied into a fixed-length buffer without bounds checking.

This vulnerability could be exploited to gain the privileges of the user running netris in client mode, if they connect to a hostile netris server.

Debian reference DSA-372-1 netris – buffer overflow

Mah-Jong

Nicolas Boullis discovered two vulnerabilities in mah-jong, a network-enabled game.

CAN-2003-0705 (buffer overflow): This vulnerability could be exploited by a remote attacker to execute arbitrary code with the privileges of the user running the mah-jong server.

CAN-2003-0706 (denial of service): This vulnerability could be exploited by a remote attacker to cause the mah-jong server to enter a tight loop and stop responding to commands.

Debian reference DSA-378-1 mah-jong – buffer overflows, denial of service

Zblast

Steve Kemp discovered a buffer overflow in zblast-svgalib, when saving the high score file. This vulnerability could be exploited by a local user to gain gid 'games', if they can achieve a high score.

Debian reference DSA-369-1 zblast – buffer overflow

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.

Exim

A buffer overflow exists in exim, which is the standard mail transport agent in Debian. By supplying a specially crafted HELO or EHLO command, an attacker could cause a constant string to be written past the end of a buffer allocated on the heap. This vulnerability is not believed at this time to be exploitable to execute arbitrary code.

Debian reference DSA-376-2 exim – buffer overflow

Autorespond

Christian Jaeger found a buffer overflow in autorespond, an email autoresponder used with qmail. This could potentially be exploited by a remote attacker to gain the privileges of a user who has configured qmail to forward messages to autorespond. This is currently not believed to be exploitable due to incidental limits on the length of the problematic input, but there may be situations in which these limits do not apply.

Debian reference DSA-373-1 autorespond – buffer overflow

PAM-pgSQL

Florian Zumbiehl reported a vulnerability in pam-pgsql where the authentication credentials are used as a format string when writing a log message. This vulnerability may allow an attacker to execute arbitrary code with the privileges of the program requesting PAM authentication.

Debian reference DSA-370-1 pam-pgsql – format string

Xtokkaetama

Another buffer overflow was discovered in xtokkaetama, involving the "-nickname" command line option. This vulnerability could be exploited by a local attacker to gain gid 'games'.

Debian reference DSA-367-1 xtokkaetama – buffer overflow

Xpcd

Steve Kemp discovered a buffer overflow in xpcd-svga which can be triggered by a long HOME environment variable. This vulnerability could be exploited by a local attacker to gain root privileges.

Debian reference DSA-368-1 xpcd – buffer overflow

PAM-smb

Dave Airlie *airlied@samba.org* discovered a vulnerability in PAM-smb. This is a PAM authentication module (and server) which makes it possible to authenticate users against a password database managed by Samba or a Microsoft Windows server.

A buffer overflow can occur if a long password is supplied. The overflow can then be exploited to execute arbitrary code with the privileges of the process that invokes the PAM services.

Debian reference DSA-374-1 libpam-smb – buffer overflow
SuSE reference SuSE-SA:2003:036
Red Hat reference RHSA-2003:261-07

Perl

Eye on Security found a cross-site scripting vulnerability in the start_form() function in CGI.pm. This function outputs user-controlled data into the action attribute of a form element without sanitizing it, allowing a remote attacker to place a web script in a URL that feeds into a form's action parameter and allows execution by the browser, as if it was coming from the site. Any program that uses this function in the CGI.pm module may be affected.

Debian reference DSA-371-1 perl – cross-site scripting
Mandrake reference MDKSA-2003:084

Wu-ftpd

Janusz Niewiadomski and Wojciech Purczynski of iSEC Security Research have found a single byte buffer overflow in the Washington University ftp daemon (wuftpd), a widely used ftp server for Linux-like systems.

The names of the files to be included are passed as command line arguments to tar, without ensuring that they cannot be interpreted as command-line options. GNU tar supports several command line options that can exploit this vulnerability to execute arbitrary programs with the privileges of the wu-ftpd process.

Georgi Guninski pointed out that this vulnerability exists in Debian woody.

Debian reference DSA-377-1 wu-ftpd – insecure program execution

Sendmail

The well known and widely used MTA is vulnerable to a remote denial-of-service attack in version 8.12.8 and earlier (but not before 8.12). The bug exists in the DNS map code. This feature is enabled by specifying FEATURE('enhdnsbl'). When sendmail receives an invalid DNS response, it tries to call free(3) on random data, which leads to a process crash.

The Common Vulnerabilities and Exposures project has assigned CAN-2003-0688 to this issue.

Red Hat reference RHSA-2003:265-05
SuSE reference SuSE-SA:2003:035

Apache

The Apache HTTP server is a powerful, full-featured, efficient Web server.

Ben Laurie found a bug in the optional renegotiation code in mod_ssl included with Apache 2 versions 2.0.35 through 2.0.46 that can cause cipher suite restrictions to be ignored. This is triggered if optional renegotiation is used (SSLOptions +OptRenegotiate) along with verification of client certificates and a change to the cipher suite over the renegotiation. The Common Vulnerabilities and Exposures project has assigned CAN-2003-0192 to this issue.

Yoshioka Tsuneo found that Apache 2 versions 2.0.35 to 2.0.46 have a bug that can cause a remote Denial of Service. When a client requests that proxy ftp connect to a ftp server with an IPv6 address, and the proxy is unable to create an IPv6 socket, an infinite loop occurs. The Common Vulnerabilities and Exposures project has assigned CAN-2003-0254 to this issue.

Saheed Akhtar found that Apache 2 versions 2.0.35 through 2.0.46 have a bug in the prefork MPM when handling accept errors. In a server with multiple listening sockets, a certain error returned by accept() on a rarely-accessed port can cause a temporary denial of service. This has a Common Vulnerabilities and Exposures project number CAN-2003-0253.

Apache 2 could enter an infinite loop handling internal redirects and nested subrequests (VU#379828). A patch for this issue adds the new LimitInternalRecursion directive.

Red Hat reference RHSA-2003:240-09
Mandrake reference MDKSA-2003:075-1

GDM

GDM is the GNOME Display Manager for X.

Several vulnerabilities were discovered in versions of GDM prior to 2.4.1.6. The first vulnerability is that any user can read any text file on the system, as code originally written to be run as the user logging in was in fact being run as the root user. This code allows the examination of the ~/.xsession-errors file.

If a user creates a symlink from this file to any other file on the system during the session, and ensures that the session lasts less than ten seconds, the user can read the file, provided it is a readable text file. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0547 to this issue.

Another two vulnerabilities were found in the XDMCP code that could be exploited to crash the main gdm daemon. The crash would prevent new sessions from launching (but without affecting the current session).

The first problem here is caused by the indirect query structure being used immediately after being freed, due to a missing 'continue' statement in a loop; this happens if a choice of server expired and the client tried to connect.

The second XDMCP problem is caused by a failure to check the length of the authorization data being checked as a string. If there are less than 18 bytes of data, the daemon can overrun the end of the string by a few bytes in the strncmp, which could cause a SEGV.

Red Hat reference RHSA-2003:258-11
Mandrake reference MDKSA-2003:085
SuSE reference SuSE-SA:2003:032

GtkHTML

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

Versions of GtkHTML prior to 1.1.10 contain a bug when handling HTML messages. Alan Cox discovered that certain malformed messages could cause the Evolution mail component to crash due to a null pointer dereference in the GtkHTML library. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0541 to this issue.

Red Hat reference RHSA-2003:264-11