Insecurity News

mod_python

mod_python embeds the Python language interpreter within the Apache httpd server. The Apache Software Foundation found that some versions of mod_python versions 3.0.3 and earlier contain a bug which, when processing a request with a malformed query string, could cause the corresponding Apache child to crash. This bug could be exploited by a remote attacker to cause a denial of service. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0973 to this issue.

Red Hat reference RHSA-2004:063-02
Debian reference DSA-452-1 libapache-mod-python -- denial of service

Xboing

Steve Kemp has discovered a number of buffer overflow bugs in xboing, a game, which could be exploited by a local attacker to gain gid "games".

Debian reference DSA-451-1 xboing -- buffer overflows

hsftp

Ulf Härnhammar found a format string vulnerability in hsftp. This vulnerability could be exploited by an attacker able to create files on a remote server with carefully crafted names, to which a malicious user would connect using hsftp. When the user requests a directory listing, particular bytes in memory could be overwritten, potentially allowing arbitrary code to be executed with the privileges of the user invoking hsftp.

Debian reference DSA-447-1 hsftp -- format string

Lbreakout2

Ulf Härnhammar discovered a vulnerability in lbreakout2, a game, where proper bounds checking was not performed on environment variables. This bug could be exploited by a local attacker to gain the privileges of group "games".

Debian reference DSA-445-1 lbreakout2 -- buffer overflow

Security Posture of Major Distributions

Distributor	Security Sources	Comments
Debian	Info: *http://www.debian.org/security/* List: *http://lists.debian.org/debian-security-announce/* Reference: DSA-... 1)	The current Debian security advisories are included on the homepage. Advisories are provided as HTML pages with links to the patches. The security advisory also contains a reference to the mailing list.
Gentoo	Forum: *http://forums.gentoo.org/* List: *http://www.gentoo.org/main/en/lists.xml* Reference: GLSA: ... 1)	Unfortunately, Gentoo does not offer a website with security updates or other security information. This forum is the only alternative.
Mandrake	Info: *http://www.mandrakesecure.net* List: *http://www.mandrakesecure.net/en/mlist.php* Reference: MDKSA-... 1)	MandrakeSoft runs its own Web site on security topics. Among other things, it includes security advisories and references to the mailing lists. The advisories are HTML pages, but there are no links to the patches.
Red Hat	Info: *http://www.redhat.com/errata/* List: *http://www.redhat.com/mailing-lists/* Reference: RHSA-... 1)	Red Hat files security advisories as so-called Errata: Issues for each Red Hat Linux version are then grouped. The security advisories are provided in the form of an HTML page with links to patches.
Slackware	Info: *http://www.slackware.com/security/* List: *http://www.slackware.com/lists/* (slackware-security) Reference: [slackware-security] ... 1)	The start page contains links to the security mailing list archive. No additional information on Slackware security is available.
Suse	Info: *http://www.suse.de/uk/private/support/security/* Patches: *http://www.suse.de/uk/private/download/updates/* List: suse-security-announce Reference: SUSE-SA ... 1)	There is no longer a link to the security page after changes to the Web site. It contains information on the mailing list and the advisories. The security patches for the individual Suse Linux versions are shown in red on the general updates site. A short description of the vulnerability the patch resolves is provided

1) All distributors indicate security mails in the subject line.

cgiemail

A vulnerability was discovered in cgiemail, a CGI program used to email the contents of an HTML form, whereby it could be used to send email to arbitrary addresses. This type of vulnerability is commonly exploited to send unsolicited commercial email (spam).

Debian reference DSA-437-1 cgiemail -- open mail relay

Synaesthesia

Ulf Härnhammar discovered a flaw in synaesthesia, a program which represents sounds visually. Synaesthesia created its configuration file while holding root privileges, allowing a local user to create files owned by root and writable by the user's primary group. This type of vulnerability can usually be easily exploited to execute arbitrary code with root privileges.

Debian reference DSA-446-1 synaesthesia -- insecure file creation

libxml2

Yuuichi Teranishi discovered a vulnerability in libxml prior to 2.6.6, the GNOME XML library. When fetching a remote resource via FTP or HTTP, the libxml2 library uses special parsing routines which can, if passed a very long URL, cause a buffer overflow. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0110 to this issue.

Mandrake reference MDKSA-2004:018
Red Hat reference RHSA-2004:091-07
Debian reference DSA-455-1 libxml -- buffer overflows

mutt

Mutt is a popular text-mode mail user agent. A new vulnerability in the index menu code within mutt was reported by Neils Heinen that could theoretically allow a remote malicious attacker to send a carefully crafted mail message that can cause mutt to segfault and, as a result, possibly execute arbitrary code as the user running mutt. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0078 to this issue.

Mandrake reference MDKSA-2004:010
Red Hat reference RHSA-2004:051-05

mtools

Sebastian Krahmer has found a flaw within the mtools package. The mformat program, when installed suid root, can create any file with 0666 permissions as root. In addition, it does not drop privileges when reading local configuration files. ■

Mandrake reference MDKSA-2004:016

pwlib

PWLib is a cross-platform class library which is designed to support the OpenH323 project. The NISCC uncovered flaws in pwlib prior to version 1.6.0 via a test suite for the H.225 protocol. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0097 to this issue.

An attacker could trigger these bugs by sending carefully crafted messages to an application. The effects of such an attack can vary depending on the application, but would usually result in a Denial of Service (DoS). ■

Mandrake reference MDKSA-2004:017
Red Hat reference RHSA-2004:048-03
Debian reference DSA-448-1 pwlib -- several vulnerabilities

Metamail

Ulf Härnhammar discovered two format string bugs in Metamail, a MIME implementation. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0104 to this issue.

He discovered a further two buffer overflow bugs in metamail. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0105 to this issue.

An attacker can theoretically create a carefully-crafted mail message which will execute arbitrary code as the victim when it is opened and parsed through metamail. ■

Mandrake reference MDKSA-2004:014
Debian reference DSA-449-1 metamail -- buffer overflow, format string bugs

xf86/XFree86

XFree86 is an open-source implementation of the X Window System that acts as a client-server-based API between different hardware components like display, mouse, keyboard and so on. Two buffer overflow vulnerabilities were found by iDEFENSE in XFree86's parsing of the font.alias file.

The X server, which runs as root, fails to check the length of user-provided input; as a result a malicious local attacker could exploit this vulnerability by creating a carefully-crafted file and gaining root privileges, which could eventually lead to the execution of arbitrary code. Additional vulnerabilities were found by David Dawes, also in the reading of font files.

The Common Vulnerabilities and Exposures project has assigned the names CAN-2004-0083 and CAN-2004-0084 to these issues. David Dawes has discovered some additional flaws in reading font files. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0106 to these issues.

Additional problems are CAN-2003-0690: xdm does not verify whether the pam_setcred function call succeeds, which may allow attackers to gain root privileges by triggering error conditions within PAM modules, as demonstrated in certain configurations of the MIT pam_krb5 module. CAN-2004-0093, CAN-2004-0094: Denial-of-service attacks against the X server by clients using the GLX extension and Direct Rendering Infrastructure are possible due to unchecked client data (out-of-bounds array indexes [CAN-2004-0093] and integer signedness errors [CAN-2004-0094]).

Exploitation of CAN-2004-0083, CAN-2004-0084, CAN-2004-0106, CAN-2004-0093 and CAN-2004-0094 would require a connection to the X server. By default, display managers in Debian start the X server with a configuration which only accepts local connections, but if the configuration is changed to allow remote connections, or X servers are started by other means, then these bugs could be exploited remotely.

Since the X server usually runs with root privileges, these bugs could potentially be exploited to gain root privileges. No attack vector for CAN-2003-0690 is known at this time. ■

Suse reference SuSE-SA:2004:006
Mandrake reference MDKSA-2004:012
Red Hat reference RHSA-2004:059-19
Debian reference DSA-443-1 xfree86 -- several vulnerabilities

Linux Kernel

Paul Starzetz and Wojciech Purczynski of isec.pl discovered a critical security vulnerability in the memory management code of the Linux kernel, versions 2.4.24, inside the mremap(2) system call. The do_mremap() function of the Linux Kernel is used to manage Virtual Memory Areas (VMAs) which includes the moving, removing and resizing of memory areas. To remove old memory areas do_mremap() uses the function du_munmap() without first checking the return value.

By forcing do_munmap() to return an error, the memory management of a process can be tricked into moving page table entries from one VMA to another. The destination VMA may be protected by a different ACL which enables a local attacker to gain write access to previous read-only pages. The result of this vulnerability will be a compromised system with local root access to the system. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0077 to this issue.

The Vicam USB driver in kernel versions prior to 2.4.25 does not use the copy_from_user function to access user-space, which crosses security boundaries and allows local users to cause Denial of Service (DoS) issues. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0075 to this issue.

Arjan van de Ven has found a bug in ncp_lookup() in ncpfs that could allow local privilege escalation via buffer overflow. ncpfs is used to allow a system to mount volumes of NetWare servers or print to NetWare printers. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0010 to this issue.

Alan Cox found issues in the R128 Direct Render Infrastructure that could allow local privilege escalation. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0003 to this issue. ■

Suse reference SuSE-SA:2004:005
Mandrake reference MDKSA-2004:015
Red Hat reference RHSA-2004:065-05
Debian reference DSA-453-1 linux-kernel-2.2.20-i386+m68k+powerpc -- failing function and TLB flush