INSECURITY NEWS

PHP

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

Flaws including possible information disclosure, double free, and negative reference index array underflow were found in the deserialization code of PHP. The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-1019 to this issue.

A flaw in the exif extension of PHP was found, which could lead to a stack overflow. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-1065 to this issue.

An information disclosure bug was discovered in the parsing of "GPC" variables in PHP (query strings or cookies, and POST form data). If particular scripts used the values of the GPC variables, portions of the memory space of an httpd child process could be revealed to the client. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0958 to this issue.

A file access bug was discovered in the parsing of "multipart/form-data" forms used by PHP scripts that allow file uploads. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0959 to this issue.

Flaws were found in shmop_write, pack, and unpack PHP functions. These functions are not normally passed user supplied data, so would require a malicious PHP script to be exploited. The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-1018 to this issue.

Various issues were discovered in the use of the "select" system call in PHP, which could be triggered if PHP is used in an Apache configuration.

The "phpize" shell script included in PHP can be used to build third-party extension modules. A build issue was discovered in the "phpize" script on some 64-bit platforms which prevented correct operation.

The "pcntl" extension module is now enabled in the command line PHP interpreter, /usr/bin/php. This module enables process control features such as "fork" and "kill" from PHP scripts.

Gentoo reference: GLSA 200412-14 / PHP
Red Hat reference: RHSA-2004:687-05

Samba

Samba provides file and printer sharing services to SMB/CIFS clients.

Greg MacManus of iDEFENSE Labs has discovered an integer overflow bug in Samba versions prior to 3.0.10. An authenticated remote user could exploit this bug, which may lead to arbitrary code execution on the Samba server. The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-1154 to this issue.

Users of Samba should upgrade install updates.

Gentoo reference: GLSA 200412-13 / Samba
Mandrake reference: MDKSA-2004:158
Red Hat reference: RHSA-2004:670-10
Suse reference: SUSE-SA:2004:045

Zip

The zip program is an archiving utility that can create ZIP-compatible archives.

A buffer overflow bug has been discovered in zip when handling long file names. An attacker could create a specially crafted path that could cause zip to crash or execute arbitrary instructions. The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-1010 to this issue.

Debian reference: DSA-624-1
Red Hat reference: RHSA-2004:634-08

nfs-utils

The nfs-utils package provides a daemon for the kernel NFS server and related tools, providing a much higher level of

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	Info: http://www.gentoo.org/security/en/glsa/index.xml Forum: *http://forums.gentoo.org/* List: *http://www.gentoo.org/main/en/lists.xml* Reference: GLSA: ... 1)	The current security advisories for Gentoo are listed on the Gentoo security site linked off the homepage. Advisories are provided as HTML pages with the coding to emerge the corrected versions.
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.

performance than the traditional Linux NFS server used by most users.

This package also contains the showmount program. Showmount queries the mount daemon on a remote host for information about the NFS server.

SGI reported that the statd daemon did not properly handle the SIGPIPE signal. A misconfigured or malicious peer could cause statd to crash, leading to a denial of service. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-1014 to this issue.

Arjan van de Ven discovered a buffer overflow in rquotad. On 64-bit architectures, an improper integer conversion can lead to a buffer overflow. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0946 to this issue.

Gentoo reference: GLSA 200412-08 / nfs-utils

Red Hat reference: RHSA-2004:583-09

Kernel

The Linux kernel handles the basic functions of the operating system.

This advisory includes fixes for several security issues:

Petr Vandrovec discovered a flaw in the 32bit emulation code affecting the Linux 2.4 kernel on the AMD64 architecture. A local attacker could use this flaw to gain privileges. The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-1144 to this issue.

ISEC security research discovered multiple vulnerabilities in the IGMP functionality, which was backported in the Red Hat Enterprise Linux 3 kernels. These flaws could allow a local user to cause a denial of service (crash) or potentially gain privileges on the system. Where multicast applications are being used on a system, these flaws may also allow remote users to cause a denial of service. The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-1137 to this issue.

ISEC security research and Georgi Guninski independently discovered a flaw in the scm_send function in the auxiliary message layer. A local user could create a carefully crafted auxiliary message which could cause a denial of service (system hang). The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-1016 to this issue.

A floating point information leak was discovered in the ia64 architecture context switch code. A local user could use this flaw in the ia64 architecture to read register values of other processes by setting the MFH bit. The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-0565 to this issue.

Kirill Korotaev found a flaw in load_elf_binary affecting kernels prior to 2.4.26. A local user could use this flaw to create a carefully crafted binary in such a way that it would cause a denial of service (system crash). The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2004-1234 to this issue.

Red Hat reference: RHSA-2004:689-06

Suse reference: SUSE-SA:2004:044