Insecurity News

Tripwire

Tripwire is a tool that checks to see what has changed on your system. The program monitors key attributes of files that should not change, including binary signature, size, expected change of size, etc. Originally known as an intrusion detection tool, it can be used for many other purposes such as integrity assurance, change management, policy compliance and more.

Paul Herman has discovered a format string vulnerability in the tripwire program. This could allow a local user to execute arbitrary code with the rights of the user running tripwire (typically root). This vulnerability only exists when tripwire is generating an email report.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0536 to this issue.

Mandrake reference MDKSA-2004:057

xpcd

xpcd is a PhotoCD viewer. It reads the overview file with the thumbnails and you can browse the pictures. A vulnerability in xpcd-svga, part of the xpcd package, was discovered by Jaguar. xpcd-svga uses svgalib to display graphics on the console and it would copy user-supplied data of an arbitrary length into a fixed-size buffer in the pcd_open function. As well, Steve Kemp previously discovered a buffer overflow in xpcd-svga that could be triggered by a long HOME environment variable, which could be exploited by a local attacker to obtain root privileges.

The Common Vulnerabilities and Exposures project has assigned the names CAN-2004-0649 and CAN-2004-0402 to this issue.

Mandrake reference MDKSA-2004:053
Debian reference DSA-508-1 xpcd -- 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	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.

Kolab server

Luca Villani reported the disclosure of critical configuration information within Kolab, the KDE Groupware server. The affected versions store OpenLDAP passwords in plain text. The heart of Kolab is an engine written in Perl that rewrites the configuration for certain applications based on templates. The build() function in the engine left slapd.conf world-readable exhibiting the OpenLDAP root password.

Mandrake reference MDKSA-2004:052

Mod_ssl

A stack-based buffer overflow exists in the ssl_util_uuencode_binary function in ssl_engine_kernel.c in mod_ssl for the Apache webserver version 1.3.x. When mod_ssl is configured to trust the issuing CA, a remote attacker may be able to execute arbitrary code via a client certificate with a long subject DN.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0488 to this issue.

Mandrake reference MDKSA-2004:054

LHA

LHA is an archiving and compression utility for LHarc format archives. Ulf Harnhammar has discovered stack buffer overflows and directory traversal flaws.

An attacker could exploit the multiple stack-based buffer overflows in the get_header function in header.c for LHA 1.14 by creating a carefully crafted LHA archive in such a way that arbitrary code would be executed when the archive is tested or extracted by a victim. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0234 to this issue.

An attacker could exploit the multiple directory traversal issues in LHA 1.14 to allow remote attackers or local users to create arbitrary files via an LHA archive containing filenames with (1) .. sequences or (2) absolute pathnames with double leading slashes (“//absolute/path”). The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0235 to this issue.

Red Hat reference RHSA-2004:178-09
Debian reference DSA-515-1 lha -- several vulnerabilities

Krb5

Kerberos is a network authentication system. Bugs have been found in the krb5_aname_to_localname library function. Specifically, buffer overflows were possible for all Kerberos versions up to and including 1.3.3.

The krb5_aname_to_localname function translates a Kerberos principal name to a local account name, typically a UNIX username. This function is frequently used when performing authorization checks.

If configured with mappings from particular Kerberos principals to particular UNIX user names, certain functions called by krb5_aname_to_localname will not properly check the lengths of buffers used to store portions of the principal name. If configured to map principals to user names using rules, krb5_aname_to_localname would consistently write one byte past the end of a buffer allocated from the heap.

Only configurations which enable the explicit mapping or rules-based mapping functionality of krb5_aname_to_localname() are vulnerable to this problem. These configurations are not set as the default.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0523 to this issue. ■

Mandrake reference MDKSA-2004:056-1
Red Hat reference RHSA-2004:236-14

Ethereal

Ethereal is a program for monitoring and analyzing network traffic. The MMSE dissector in Ethereal releases 0.10.1 through 0.10.3 contained a buffer overflow flaw. On a system where Ethereal is running, a remote attacker could send malicious packets that could cause Ethereal to crash or execute arbitrary code. In addition, other flaws in Ethereal prior to 0.10.4 were found that could cause it to crash in response to carefully crafted SIP, AIM, or SPNEGO packets.

The Common Vulnerabilities and Exposures project has assigned the names CAN-2004-0507, CAN-2004-0504, CAN-2004-0505 and CAN-2004-0506 to this issue. ■

Red Hat reference RHSA-2004:234-06
Debian reference DSA-511-1 ethereal -- buffer overflows

CVS

The Concurrent Versions System (CVS) offers tools which allow developers to share and maintain large software projects and is frequently used to manage source code repositories.

While investigating a previously fixed vulnerability, Derek Price discovered a flaw relating to malformed "Entry" lines which lead to a missing NULL terminator. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0414 to this issue.

Stefan Esser and Sebastian Krahmer conducted an audit of CVS and fixed a number of issues that may have had security consequences. Among the issues deemed likely to be exploitable were:

- a double-free condition relating to the error_prog_name string.
- By sending a large number of arguments to the CVS server, it is possible to cause it to allocate a huge amount of memory which does not fit into the address space, causing an error .
- out-of-bounds writes in the serv_notify() function.

An attacker who has access to a CVS server may be able to execute arbitrary code under the UID on which the CVS server is executing.

The Common Vulnerabilities and Exposures project has assigned the names CAN-2004-0416, CAN-2004-0417 and CAN-2004-0418 to this issue. ■

Suse reference SuSE-SA:2004:015
Mandrake reference MDKSA-2004:058
Red Hat reference RHSA-2004:233-07
Debian reference DSA-517-1 cvs -- buffer overflow

KDElibs

The kdelibs3 package is a core package for the K desktop environment (KDE). The URI handler of the kdelibs3 and kdelibs class library contains a flaw which allows remote attackers to create arbitrary files as the user utilizing the kdelibs3/kdelibs package. This affects applications which use the kdelibs3/kdelibs URI handler such as Konqueror or Kmail.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0411 to this issue. ■

Suse reference SuSE-SA:2003:014

Squid

Squid is a web-proxy cache. The NTLM authentication helper application of Squid is vulnerable to a buffer overflow that can be exploited remotely by sending an overly long password, thus overflowing the buffer and granting the ability to execute arbitrary code. If Squid is configured to use the NTLM authentication helper, then this error could be exploited.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0541 to this issue. ■

Suse reference SuSE-SA:2004:016
Mandrake reference MDKSA-2004:059
Red Hat reference RHSA-2004:242-06

Gallery

A bug has been discovered in gallery, a web-based photo album which is written in php. With this error, a remote attacker could gain access to the gallery "admin" user without the proper authentication.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0522 to this issue. ■

Debian reference DSA-512-1 gallery -- unauthenticated access

Gatos

Steve Kemp discovered a vulnerability in xatitv, one of the programs in the gatos package, which is used to display video with certain ATI video cards.

xatitv is installed setuid root in order to gain direct access to the video hardware. It normally drops root privileges after successfully initializing itself. However, if initialization fails due to a missing configuration file, root privileges are not dropped, and xatitv executes the system(3) function to launch its configuration program without sanitizing user-supplied environment variables.

By exploiting this vulnerability, a local user could gain root privileges if the configuration file does not exist. However, a default configuration file is supplied with the package, and so this vulnerability is not exploitable unless this file is removed by the administrator.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0395 to this issue. ■

Debian reference DSA-509-1 gatos -- privilege escalation