Insecurity News

Kerberos

Kerberos is a networked authentication system that uses a trusted third party (a KDC) to authenticate clients and servers against each other.

Several double-free bugs were found in the Kerberos 5 KDC and libraries. A remote attacker could potentially exploit these flaws to execute arbitrary code. The Common Vulnerabilities and Exposures project (*http://cve.mitre.org*) has assigned the names CAN-2004-0642 and CAN-2004-0643 to these issues. A double-free bug was also found in the krb524 server (CAN-2004-0772).

An infinite loop bug was found in the Kerberos 5 ASN.1 decoder library. A remote attacker who knows about this bug may be able to trigger this flaw and cause a denial of service attack within the Kerberos network. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0644 to this issue.

When attempting to contact a KDC, the Kerberos libraries will iterate through the list of configured servers, attempting to contact each in turn. If one of the servers becomes unresponsive, the client will time out and contact the next configured server. When the library attempts to contact the next KDC, the entire process is repeated. For applications that must contact a KDC several times, the accumulated time spent waiting can become significant.

All users of krb5 should install updates that address these issues. ■

Mandrake reference: MDKSA-2004:088
Debian reference: DSA-543-1
Gentoo reference: GLSA 200409-09 / mit-krb5
Red Hat reference: RHSA-2004:350-12

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.

zlib

zlib is a widely used data compression library. Programs linked against it include most desktop applications as well as servers such as Apache and OpenSSH.

The *inflate* function of zlib handles certain input data incorrectly, which could lead to a denial of service condition for programs using it with untrusted data. Whether the vulnerability can be exploited locally or remotely depends on the application using it.

zlib versions older than version 1.2 are not affected. There is no known workaround. After applying the update all programs linked against libz must be restarted. ■

Mandrake reference: MDKSA-2004:090
SuSE reference: SUSE-SA:2004:028

Qt

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System.

During a security audit, Chris Evans discovered a heap overflow in the BMP image decoder in Qt versions prior to 3.3.3. An attacker could use this vulnerability to create a carefully crafted BMP file in such a way that it would cause an application linked with Qt to crash or possibly execute arbitrary code when the file was opened by a victim. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0691 to this issue.

Additionally, various flaws were discovered in the GIF, XPM, and JPEG decoders in Qt versions prior to 3.3.3. An attacker could create a carefully crafted image file that could cause an application linked against Qt to crash when the file was opened. The Common Vulnerabilities and Exposures project has assigned the names CAN-2004-0692 and CAN-2004-0693 to these issues.

Users of Qt should update to these updated packages that contain backported patches. ■

Mandrake reference: MDKSA-2004:085
SuSE reference: SUSE-SA:2004:027
Slackware reference: SSA:2004-236-01
Debian reference: DSA-542-1 qt -- unsanitised input
Red Hat reference: RHSA-2004:414-19

KDE

KDE is a desktop environment for Unix and Linux systems.

The integrity of symlinks used by KDE is not ensured and as a result can be abused by local attackers to create or truncate arbitrary files or to prevent KDE applications from functioning correctly (CAN-2004-0689).

The DCOP Server creates temporary files in an insecure manner. Because these temporary files are used for authentication-related purposes, a local attacker could compromise the account of any user running a KDE application (CAN-2004-0690). Note that only KDE 3.2.x is affected by this vulnerability.

Konqueror allows websites to load web pages into a frame of any other frame-based web page that the user may have open. Konqueror also allows websites to set cookies for certain country-specific top-level domains. All country-specific secondary top-level domains that use more than 2 characters in the secondary part of the domain name, and that use a secondary part other than com, net, mil, org, gove, edu, or int are affected (CAN-2004-0746) (CAN-2004-0721). ■

Mandrake references: MDKSA-2004:086
Slackware reference: SSA:2004-247-01
Debian reference: DSA-539-1 kdelibs -- temporary directory vulnerability

Acrobat

The Adobe Acrobat Reader browser is a desktop application that allows for the viewing, distributing, and printing of documents in portable document format (PDF).

iDEFENSE has reported that Adobe Acrobat Reader 5.0 provides the potential for a buffer overflow when decoding uu-encoded documents. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0631 to this issue.

iDEFENSE also reported that Adobe Acrobat Reader 5.0 contains an input validation error in its uu-encoding feature. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0630 to this issue.

All users of Acrobat Reader are advised to upgrade.

Red Hat reference: RHSA-2004:432-08

Apache

The Apache HTTP server is a powerful, full-featured, efficient, and freely-available web server.

An input filter bug in *mod_ssl* was discovered in Apache httpd version 2.0.50 and earlier. A remote attacker could force an SSL connection to be aborted in a particular state and cause an Apache child process to enter an infinite loop, consuming CPU resources. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0748 to this issue. SuSE reports the advisory CAN-2004-0751 for a related vulnerability.

If you need a solution before you have time to patch, SuSE suggests the temporary workaround of disabling the mod_ssl module in your Apache configuration and restarting the Apache process without SSL support. You also need to update the *libapr0* package and either the *apache2-prefork* or *apache2-worker* package, depending on whether you use the *-prefork* or *-worker* configuration. ■

SuSE reference: SUSE-SA:2004:030
Red Hat reference: RHSA-2004:349-10

PNG

Several different security vulnerabilities were found in the PNG library, which is used by applications to support the PNG image format.

Chris Evans reports that a remote attacker is able to execute arbitrary code by triggering a buffer overflow due to the incorrect handling within the PNG library of the length of transparency chunk data. An overflow is also possible through certain other features related to the behavior of the PNG library in image processing applications. (VU#388984, VU#817368, CAN-2004-0597) A special PNG image can be used by an attacker to cause an application to crash due to NULL pointer dereference in the function *png_handle_iCPP()* (and other locations). (VU#236656, CAN-2004-0598) Integer overflows were found in *png_handle_sPLT()*, *png_read_png()* functions, and other locations. These bugs may at least crash an application. (VU#160448, VU#477512, VU#286464, CAN-2004-0599) ■

SuSE reference: SUSE-SA:2004:023
Slackware reference: SSA:2004-222-01

Gaim

Gaim is an instant messenger client that can handle multiple protocols.

Buffer overflow bugs were found in the Gaim MSN protocol handler. In order to exploit these bugs, an attacker would have to perform a man in the middle attack between the MSN server and the vulnerable Gaim client. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0500 to this issue.

Buffer overflow bugs have been found in the Gaim URL decoder, local hostname resolver, and the RTF message parser. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0785 to this issue.

A shell escape bug has been found in the Gaim smiley theme file installation. When a user installs a smiley theme, which is contained within a tar file, the unarchiving of the data is done in an unsafe manner. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0784 to this issue.

An integer overflow bug has been found in the Gaim Groupware message receiver. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0754 to this issue. ■

SuSE reference: SUSE-SA:2004:023
Slackware reference: SSA:2004-239-01
Red Hat reference: RHSA-2004:400-15

rsync

The rsync program synchronizes files over a network.

Versions of rsync up to and including version 2.6.2 contain a path sanitization issue. This issue could allow an attacker to read or write files outside of the rsync directory. This vulnerability is only exploitable when an rsync server is enabled and is not running within a *chroot* jail. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0792 to this issue.

Users of rsync are advised to upgrade to this updated package, which contains a backported patch and is not affected by this issue. ■

SuSE reference: SUSE-SA:2004:026
Debian reference: DSA-538-1 rsync -- unsanitised input processing
Red Hat reference: RHSA-2004:436-07