Insecurity News

Kdelibs

Konqueror is a file manager and Web browser for the K Desktop Environment (KDE). Flaws have been found in the cookie path handling between a number of Web browsers and servers. The HTTP cookie standard allows a Web server supplying a cookie to a client to specify a subset of URLs on the original server to which the cookie applies.

Web servers such as Apache do not filter returned cookies and assume that the client will only send back cookies for requests that fall within the server-supplied subset of URLs. However, by supplying URLs that use path traversal (/../) and character encoding, it is possible to send the browser to an application running at /app1. The browser could inadvertently include it with a request sent to /app2 on the same server.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0592 to this issue.

Red Hat reference RHSA-2004:075-05

Debian reference DSA-459-1 kdelibs -- cookie path traversal

Sysstat

Sysstat is a tool for gathering system statistics. Alan Cox discovered that the isag utility (which graphically displays data collected by the sysstat tools), creates a temporary file without taking proper precautions. This vulnerability could allow a local attacker to overwrite files with the privileges of the user invoking isag. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0107 to this issue.

Other issues addressed in this advisory include:

- iostat -x should return all partitions on the system (up to a maximum of 1024)
- sar should handle network device names with more than 8 characters properly

Red Hat reference RHSA-2004:093-05

Debian reference DSA-460-1 sysstat -- insecure temporary file

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.

Gdk-pixbuf

The gdk-pixbuf package contains an image loading library used with the GNOME GUI desktop environment. Thomas Kristensen discovered a vulnerability in gdk-pixbuf (binary package libgdk-pixbuf2), the GdkPixBuf image library for Gtk, that can cause the surrounding application such as Evolution, to crash. This issue was caused by a flaw that affects versions of the gdk-pixbuf package prior to 0.20.

To exploit this flaw, a remote attacker could send a carefully-crafted BMP file via email, which would cause Evolution to crash. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0111 to this issue.

Red Hat reference RHSA-2004:102-03

Debian reference DSA-464-1 gdk-pixbuf -- broken image handling

Squid

Squid is a fully featured Web proxy cache. A vulnerability was discovered in squid version 2.5.STABLE4 and earlier with the processing of %-encoded characters in a URL. If a Squid configuration uses Access Control Lists (ACLs), it is possible for a remote attacker to create URLs that would not be correctly tested against Squid's ACLs, potentially allowing clients to access prohibited URLs.

New packages contain a new Access Control type, "urllogin", which can be used to protect vulnerable Microsoft Internet Explorer clients from accessing URLs that contain login information. These are often used by fraudsters to trick users into revealing personal data.

Note that the default Squid configuration does not make use of this new Access Control type. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0189 to this issue. You will need to configure Squid with ACLs that use this new type, in accordance with your own site policies.

Two other bugs were also fixed: squid-2.4.STABLE7-url_escape.patch (a buffer overrun) and squid-2.4.STABLE7-url_port.patch (a potential denial of service).

Mandrake reference MDKSA-2004:025

Red Hat reference RHSA-2004:134-05

Debian reference DSA-474-1 squid -- ACL bypass

Mozilla

Mozilla is a Web browser and mail reader. A number of vulnerabilities were discovered in Mozilla 1.4: A website could gain access to a user's authentication credentials to a proxy server. Script.prototype.freeze/thaw could allow an attacker to run arbitrary code.

Network Security Services (NSS) is a set of libraries, shiped with Mozilla, to support cross-platform development of security-enabled server applications. NISCC testing of implementations of the S/MIME protocol uncovered a number of bugs in NSS versions prior to 3.9.

The S/MIME implementation would allow remote attackers to cause a Denial of Service and execute arbitrary code via an S/MIME email message containing certain unexpected ASN.1 constructs.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0564 to this issue.

Andreas Sandblad discovered a cross-site scripting issue. When linking to a new page it is still possible to interact with the old page before the new page has been successfully loaded. Any Javascript events will be invoked in the context of the new page, making cross-site scripting possible if the different pages belong to different domains. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0191 to this issue.

Finally, Corsaire discovered that a number of HTTP user agents contained a flaw in how they handle cookies. The HTTP cookie standard allows a Web server supplying a cookie to a client to specify a subset of URLs on the original server to which the cookie applies. Web servers such as Apache do not filter returned cookies and assume that the client will only send back cookies for requests that fall within the server-supplied subset of URLs.

However, by supplying URLs that use path traversal (/../) and character encoding, it is possible to fool many browsers into sending a cookie to a path outside of the originally-specified subset. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0594 to this issue.

Mandrake reference MDKSA-2004:021
Red Hat reference RHSA-2004:112-09

Ethereal

Ethereal is a program for monitoring network traffic. Stefan Esser reported that Ethereal versions 0.10.1 and earlier contain thirteen buffer overflows in the IGRP, PGM, Metflow, ISUP, TCAP, or IGAP dissectors. On a system where Ethereal is being run, a remote attacker could send malicious packets that could cause Ethereal to crash or execute arbitrary code.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0176 to this issue.

Jonathan Heusser discovered that a carefully-crafted RADIUS packet could cause Ethereal to crash. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0365 to this issue.

Ethereal 0.8.13 to 0.10.2 allows remote attackers to cause a Denial of Service (crash) via a zero-length Presentation protocol selector.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0367 to this issue.

It is possible, through the exploitation of some of these vulnerabilities, to cause Ethereal to crash or run arbitrary code by injecting a malicious, malformed packet onto the wire, by convincing someone to read a malformed packet trace file, or by creating a malformed color filter file.

Mandrake reference MDKSA-2004:024
Red Hat reference RHSA-2004:137-07

Mplayer

A remotely exploitable buffer overflow vulnerability was found in MPlayer. A malicious host can craft a harmful HTTP header ("Location:"), and trick MPlayer into executing arbitrary code upon parsing that header.

Mandrake reference MDKSA-2004:026

Oftpd

Oftpd is an anonymous FTP server. A vulnerability was discovered in oftpd whereby a remote attacker could cause the oftpd process to crash by specifying a large value in a PORT command. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0376 to this issue.

Debian reference DSA-473-1 oftpd -- denial of service

Pam-pgsql

Pam-pgsql is a PAM module to authenticate using a PostgreSQL database. Primoz Bratanic discovered a vulnerability in libpam-psgl. The library does not escape all user-supplied data that are sent to the database. An attacker could exploit this bug to insert SQL statements. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0366 to this issue.

Debian reference DSA-469-1 pam-pgsql -- missing input sanitising

OpenSSL

OpenSSL is a toolkit that implements Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a strong general purpose cryptography library. Testing performed by the OpenSSL group using the Codenomicon TLS Test Tool discovered a null-pointer assignment in the do_change_cipher_spec() function in OpenSSL 0.9.6c-0.9.6k and 0.9.7a-0.9.7c.

A remote attacker could perform an SSL/TLS handshake against a server that used the OpenSSL library in such a way as to cause OpenSSL to crash. Depending on the application this could lead to a Denial of Service (DoS). The Common Vulnerabilities and Exposures project has assigned CAN-2004-0079 to the issue.

Another bug was found by Stephen Henson in OpenSSL versions 0.9.7a-0.9.7c; there is a flaw in the SSL/TLS handshaking code when using Kerberos ciphersuites. A remote attacker could use an SSL/TLS handshake against a server configured to use Kerberos ciphersuites to cause OpenSSL to crash.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0112 to this issue.

Testing performed by the OpenSSL group using the Codenomicon TLS Test Tool uncovered a bug in OpenSSL 0.9.6 prior to 0.9.6d that can lead to a Denial of Service attack (infinite loop).

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0081 to this issue.

Suse reference SuSE-SA:2004:007
Mandrake reference MDKSA-2004:023
Red Hat reference RHSA-2004:121-04
Debian reference DSA-465-1 openssl -- several vulnerabilities