Insecurity News

kdebase

The KDE team discovered a vulnerability in the way KDE uses Ghostscript software when processing PostScript (PS) and PDF files.

An attacker could provide a malicious PostScript or PDF file via mail or websites that could lead to executing arbitrary commands under the privileges of the user viewing the file or when the browser generates a directory listing with thumbnails.

Debian reference DSA-296-1 kdebase – insecure execution

rinetd

Sam Hocevar discovered a security problem in rinetd, an IP connection redirection server. When the connection list is full, rinetd resizes the list in order to store the new incoming connection. However, this is done improperly, resulting in a denial of service and potentially execution of arbitrary code.

Debian reference DSA-289-1 rinetd – incorrect memory resizing

sendmail-wide

Michal Zalewski discovered a buffer overflow, triggered by a char to int conversion, in the address parsing code in sendmail, a widely used powerful, efficient, and scalable mail transport agent. This problem is potentially remotely exploitable.

Debian reference DSA-290-1 sendmail-wide – char-to-int conversion

lprng

Karol Lewandowski discovered that psbanner, a printer filter that creates a PostScript format banner that is part of LPRng, insecurely creates a temporary file for debugging purpose when it is configured as filter. The program does not check whether this file already exists or is linked to another place, psbanner writes its current environment and called arguments to the file unconditionally with the user id daemon.

Debian reference DSA-285-1 lprng – insecure temporary file

Security Posture of Major Distributions

Distributor	Security Sources	Comment
Debian	Info: *www.debian.org/security/*, List: debian-security-announce, Reference: DSA-... [1)]	Debian have integrated current security advisories on their web site. The advisories take the form of HTML pages with links to patches. The security page also contains a note on the mailing list.
Mandrake	Info: *www.mandrakesecure.net*, List: security-announce, Reference: MDKSA-... [1)]	MandrakeSoft run a web site dedicated to security topics. Amongst other things the site contains security advisories and references to mailing lists. The advisories are HTML pages,but there are no links to the patches.
Red Hat	Info: *www.redhat.com/errata/* List: *www.redhat.com/mailing-lists/* (linux-security and redhat-announce-list) Reference: RHSA-... [1)]	Red Hat categorizes security advisories as Errata: Under the Errata headline any and all issues for individual Red Hat Linux versions are grouped and discussed. The security advisories take the form of HTML pages with links to patches.
SCO	Info: *www.sco.com/support/security/*, List: *www.sco.com/support/forums/announce.html*, Reference: CSSA-... [1)]	You can access the SCO security page via the support area. The advisories are provided in clear text format.
Slackware	List: *www.slackware.com/lists/* (slackware-security), Reference: slackware-security ...[1)]	Slackware do not have their own security page, but do offer an archive of the Security mailing List.
SuSE	Info: *www.suse.de/uk/private/support/security/*, Patches: *www.suse.de/uk/private/download/updates/*, List: suse-security-announce, Reference: suse-security-announce ... [1)]	There is a link to the security page on the homepage. The security page contains information on the mailing list and advisories in text format. Security patches for individual SuSE Linux versions are marked red on the general update page and comprise a short description of the patched vulnerability.

[1)] Security mails are available from all the above-mentioned distributions via the reference provided.

mime-support

Colin Phipps discovered several problems in mime-support, that contains support programs for the MIME control files 'mime.types' and 'mailcap'. When a temporary file is created it is done so in an insecure way, allowing an attacker to overwrite arbitrary under the user id of the person executing run-mailcap.

Also, when run-mailcap is executed on a file with a potentially problematic filename, a temporary file is created (securely this time), removed and a symbolic link to this filename is created. An attacker could recreate the file before the symbolic link is created, forcing the display program to display different content.

Debian reference DSA-292-3 mime-support – insecure temporary file creation

snort

Two vulnerabilities have been discovered in Snort, a popular network intrusion detection system. Snort comes with modules and plugins that perform a variety of functions such as protocol analysis. The following issues have been identified:

- Heap overflow in Snort "stream4" pre-processor (VU#139129, CAN-2003-0209, Bugtraq Id 7178)
  Researchers at CORE Security Technologies have discovered a remotely exploitable integer overflow that results in overwriting the heap in the "stream4" pre-processor module. This module allows Snort to reassemble TCP packet fragments for further analysis. An attacker could insert arbitrary code that would be executed as the user running Snort, probably root.
- Buffer overflow in Snort RPC pre-processor (VU#916785, CAN-2003-0033, Bugtraq Id 6963)
  Researchers at Internet Security Systems X-Force have discovered a remotely exploitable buffer overflow in the Snort RPC pre-processor module. Snort incorrectly checks the lengths of what is being normalized against the current packet size. An attacker could exploit this to execute arbitrary code under the privileges of the Snort process, again, probably root.

Debian reference DSA-297-1 snort – integer overflow, buffer overflow

openssl

Researchers discovered two flaws in OpenSSL, a Secure Socket Layer (SSL) library and cryptographic tools. Applications that are linked against this library are generally vulnerable to attacks that could leak the server's private key or make the encrypted session decryptable otherwise. The Common Vulnerabilities and Exposures (CVE) project identified the following vulnerabilities:

- CAN-2003-0147 OpenSSL does not use RSA blinding by default, which allows local and remote attackers to obtain the server's private key.
- CAN-2003-0131 The SSL allows remote attackers to perform an unauthorized RSA private key operation that causes OpenSSL to leak information regarding the relationship between ciphertext and the associated plaintext.

Debian reference DSA-288-1 openssl – several vulnerabilities

gkrellm-newsticker

Brian Campbell discovered two security-related problems in gkrellm-newsticker, which provides a news ticker from RDF feeds. The CVE project identifies the following problems:

- CAN-2003-0205 It can launch a web browser of the user's choice when the ticker title is clicked by using the URI given by the feed. Special shell characters are not properly escaped enabling a malicious feed to execute arbitrary shell commands.
- CAN-2003-0206 It crashes the entire gkrellm system on feeds where link or title elements are not entirely on a single line. A malicious server could craft a denial of service (DoS).

Debian reference DSA-294-1 gkrellm-newsticker – missing quoting, incomplete parser

ethereal

A vulnerability was found in Ethereal 0.9.9 and earlier that allows a remote attacker to use specially crafted SOCKS packets to cause a DoS and possibly execute arbitrary code.

A similar vulnerability exists in the NTLMSSP code in Ethereal, due to a heap-based buffer overflow.

Mandrake reference MDKSA-2003:051 : ethereal

apache2

A memory leak was discovered in Apache 2.0 through 2.0.44 that can allow a remote attacker to cause a significant denial of service (DoS) by sending requests containing a lot of linefeed characters to the server.

In addition to this, Apache does not filter terminal escape sequences from its log files, which could make it easy for an attacker to insert those sequences into the error and access logs, which could possibly be viewed by certain terminal emulators with vulnerabilities related to escape sequences.

Mandrake reference MDKSA-2003:050 : apache2

xfsdump

A vulnerability was discovered in xfsdump by Ethan Benson related to filesystem quotas on the XFS filesystem. When xfsdump runs xfsdq to save the quota information into a file at the root of the filesystem being dumped, the file is created in an unsafe manner.

A new option to xfsdq was added when fixing this vulnerability: '-f path'. This specifies an output file to use instead of the default output stream. If the file exists already, xfsdq will abort and if the file doesn't already exist, it will be created with more appropriate access permissions.

Mandrake reference MDKSA-2003:047 : xfsdump

RHN Notification Tool

An updated version of the RHN Notification Tool is now available to fix several UI and behavior bugs, as well as a memory leak.

The Red Hat Network (RHN) Notification Tool is a desktop panel applet that provides a convenient way to update your system with current errata and bug fixes from Red Hat.

A memory leak in the RHN Notification Tool that occurred when scanning the RPM database has been addressed. Additionally, some versions of the RHN Notification Tool handled network disconnection incorrectly. Other small enhancements to the applet behavior are also included in this update.

Red Hat reference RHBA-2003:080-10

glibc

The glibc packages contain standard libraries that are used by many programs. The following bugs have now been fixed: - pthread_cond_wait() which could cause program hangs in some cases - pthread_cond_timedwait() which could lead to crashes during pthread_exit or thread cancellation - Problems with destructors registered with pthread_key_create() - glibc 2.0.x compatibility was missing

Red Hat reference RHBA-2003:136-07

Samba

Digital Defense Inc. have discovered a buffer overflow in the samba file server.

The flaw allows a remote attacker to execute arbitrary commands as root on a server that runs a vulnerable version of samba. The vulnerability is known as DDI trans2.c overflow bug and has been assigned the CVE ID CAN-2003-0201. As this was found during an analysis of an exploit in the wild, it should be assumed that it is circulating on the Internet.

A possible workaround is to restrict access using the "hosts allow" directive in the smb.conf file to a group of trusted hosts/addresses that should be able to access the server. Please see the sbm.conf(5) manpage ("man smb.conf") for more details about such configuration changes. It should be noted that each change of the configuration requires restarting/reloading the samba daemon ("rcsmb reload").

The only efficient and permanent remedy for the vulnerability should be to install the provided update packages

SuSE reference SuSE-SA:2003:025

pam_xauth

Andreas Beck found a vulnerability: On Red Hat Linux including 8.0, PAM comes with a module pam_xauth which can forward X MIT-Magic-Cookies to newly instantiated sessions.

While this is generally harmless in the case of an unprivileged user that elevates his privileges to root using su or the various wrappers for some root-only programs, it does pose a security risk for root, if root uses su in order to assume the id of a less privileged user, for troubleshooting purposes and alike.

CERT Vulnerability Note VU#911505