Insecurity News

smb2www

Robert Luberda found a security problem in smb2www, a Windows Network client that is accessible through a web browser. This could lead a remote attacker to execute arbitrary programs under the user id www-data on the host where smb2www is running.

This problem has been fixed in version 980804-16.1 for the current stable distribution (woody), in version 980804-8.1 of the old stable distribution (potato) and in version 980804-17 for the unstable distribution (sid).

Debian reference DSA-203-1 smb2www

freeswan

Bindview discovered a problem in several IPSEC implementations that do not properly handle certain very short packets. IPSEC is a set of security extensions to IP which provide authentication and encryption. Free/SWan in Debian is affected by this and is said to cause a kernel panic.

This problem has been fixed in version 1.96-1.4 for the current stable distribution (woody) and in version 1.99-1 for the unstable distribution (sid). The old stable distribution (potato) does not contain Free/SWan packages.

Debian reference DSA-201-1 freeswan

kdelibs

The KDE team has discovered a vulnerability in the support for various network protocols via the KIO. The implementation of the rlogin and telnet protocols allows a carefully crafted URL in an HTML page, HTML email or other KIO-enabled application to execute arbitrary commands on the system using the victim's account on the vulnerable computer system.

This problem has been fixed by disabling rlogin and telnet in version 2.2.2-13.woody.5 for the current stable distribution (woody). The old stable distribution (potato) is not affected since it doesn't contain KDE. A correction for the package in the unstable distribution (sid) is not yet available.

Debian reference DSA-204-1 kdelibs

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.

im

Tatsuya Kinoshita discovered that IM, which contains interface commands and Perl libraries for E-mail and NetNews, creates temporary files insecurely.

The impwagent program creates a temporary directory in an insecure manner in /tmp using predictable directory names without checking the return code of mkdir, so it's possible to seize a permission of the temporary directory by local access as another user.

The immknmz program creates a temporary file in an insecure manner in /tmp using a predictable filename, so an attacker with local access can easily create and overwrite files as another user.

These problems have been fixed in version 141-18.1 for the current stable distribution (woody), in version 133-2.2 of the old stable distribution (potato) and in version 141-20 for the unstable distribution (sid).

Debian reference DSA-202-1 im

kernel

The kernel in Red Hat Linux 7.1, 7.1K, 7.2, 7.3, and 8.0 is vulnerable to a local denial of service attack. Updated packages are available which address this vulnerability, as well as bugs in several drivers.

The Linux kernel handles the basic functions of the operating system. A vulnerability in the Linux kernel has been discovered in which a non-root user can cause the machine to freeze. This kernel addresses the vulnerability.

Note: This bug is specific to the x86 architecture kernels only, and does not affect ia64 or other architectures.

In addition, a bug in the maestro3 soundcard driver has been fixed as well as a bug in the xircom pcmcia driver network driver and the tg3 network driver for Broadcom gigabit ethernet chips. All users of Red Hat Linux 7.1, 7.1K, 7.2, 7.3, and 8.0 should upgrade to the errata packages.

Thanks go to Christopher Devine for reporting the vulnerability on bugtraq, and Petr Vandrovec for being the first to supply a fix to the community.

Red Hat reference RHSA-2002:262-07

kerberos

A remotely exploitable stack buffer overflow has been found in the Kerberos v4 compatibility administration daemon.

Kerberos is a network authentication system. A stack buffer overflow has been found in the implementation of the Kerberos v4 compatibility administration daemon (kadmind4), which is part of the the MIT krb5 distribution.

This vulnerability is present in version 1.2.6 and earlier of the MIT krb5 distribution and can be exploited to gain unauthorized root access to a KDC host.

The attacker does not need to authenticate to the daemon to successfully perform this attack. kadmind4 is included in the Kerberos packages in Red Hat Linux 6.2, 7, 7.1, 7.2, 7.3, and 8.0, but by default is not enabled or used.

All users of Kerberos are advised to upgrade to the errata packages which contain a backported patch.

Red Hat reference RHSA-2002:242-06

xinetd

Xinetd contains a denial-of-service (DoS) vulnerability. UPDATE 2002-12-02: Updated packages are available to fix issues encountered with the previous errata packages.

Xinetd is a secure replacement for inetd, the Internet services daemon.

Versions of Xinetd prior to 2.3.7 leak file descriptors for the signal pipe to services that are launched by xinetd. This could allow an attacker to execute a DoS attack via the pipe. The Common Vulnerabilities and Exposures project has assigned the name CAN-2002-0871 to this issue. Red Hat Linux 7.3 shipped with xinetd version 2.3.4 and is therefore vulnerable to this issue.

Thanks to Solar Designer for discovering this issue.

Red Hat reference RHSA-2002:196-19

WindowMaker

Al Viro discovered a vulnerability in the WindowMaker window manager. A function used to load images, for example when configuring a new background image or previewing themes, contains a buffer overflow.

The function calculates the amount of memory necessary to load the image by doing some multiplication but does not check the results of this multiplication, which may not fit into the destination variable, resulting in a buffer overflow when the image is loaded.

Mandrake reference MDKSA-2002:085

OpenLDAP

The SuSE Security Team reviewed critical parts of the OpenLDAP package. SuSE found several buffer overflows and other bugs remote attackers could exploit to gain access on systems running vulnerable LDAP servers. In addition to these bugs, various local exploitable bugs within the OpenLDAP2 libraries (open ldap2-devel package) have been fixed.

Since there is no workaround possible except shutting down the LDAP server, we strongly recommend an update. Please download the update package for your distribution and install it, using the command “rpm -Fhv file.rpm”.

The packages are being offered to install from the SuSE maintenance web. To be sure the update takes effect you have to restart the LDAP server by executing the following command as the root user:

```
/etc/rc.d/ldap restart
```

SuSE reference SuSE-SA:2002:047

samba

A vulnerability in samba versions 2.2.2 through 2.2.6 was discovered by the Debian samba maintainers.

A bug in the length checking for encrypted password change requests from clients could be exploited using a buffer overrun attack on the smbd stack. This attack would have to be crafted in such a way that converting a DOS codepage string to little endian UCS2 unicode would translate into an executable block of code.

This vulnerability has been fixed in samba version 2.2.7, and the updated packages have had a patch applied to fix the problem.

Mandrake reference MDKSA-2002:081