Insecurity News

micq

Rüdiger Kuhlmann, upstream developer of mICQ, a text based ICQ client, discovered a problem in mICQ. Receiving certain ICQ message types that do not contain the required 0xFE separator causes all versions to crash.

For the current stable distribution (woody) this problem has been fixed in version 0.4.9-0woody3. For the old stable distribution (potato) this problem has been fixed in version 0.4.3-4.1. For the unstable distribution (sid) this problem has been fixed in version 0.4.9.4-1.

Debian reference DSA-211-1 micq

perl

A security hole has been discovered in Safe.pm which is used in all versions of Perl. The Safe extension module allows the creation of compartments in which perl code can be evaluated in a new namespace and the code evaluated in the compartment cannot refer to variables outside this namespace.

However, when a Safe compartment has already been used, there's no guarantee that it is safe any longer, because there is a way for code to be executed within the Safe compartment to alter its operation mask. Thus, programs that use a Safe compartment only once are not affected by this bug.

This problem has been fixed in version 5.6.1-8.2 for the current stable distribution (woody), in version 5.004.05-6.2 and 5.005.03-7.2 for the old stable distribution (potato) and in version 5.8.0-14 for the unstable distribution (sid).

Debian reference DSA-208-1 perl

tetex-bin

The SuSE security team discovered a vulnerability in kpathsea library (libkpathsea) which is used by xdvi and dvips. Both programs call the system() function insecurely, which allows a remote attacker to execute arbitrary commands via cleverly crafted DVI files.

If dvips is used in a print filter, this allows a local or remote attacker with print permission execute arbitrary code as the printer user (usually lp).

This problem has been fixed in version 1.0.7+20011202-7.1 for the current stable distribution (woody), in version 1.0.6-7.3 for the old stable distribution (potato) and in version 1.0.7+20021025-4 for the unstable distribution (sid).

xdvik-ja and dvipsk-ja are vulnerable as well, but link to the kpathsea library dynamically and will automatically be fixed after a new libkpathsea is installed.

Debian reference DSA-207-1 tetex-bin

dhcpcd

Simon Kelly discovered a vulnerability in dhcpcd, an RFC2131 and RFC1541 compliant DHCP client daemon, that runs with root privileges on client machines.

A malicious administrator of the regular or an mistrusted DHCP server may execute any command with root privileges on the DHCP client machine by sending the command enclosed in shell metacharacters in one of the options provided by the DHCP server.

This problem has been fixed in version 1.3.17pl2-8.1 for the old stable distribution (potato) and in version 1.3.22pl2-2 for the testing (sarge) and unstable (sid) distributions. The current stable distribution (woody) does not contain a dhcpcd package.

Debian reference DSA-219-1 dhcpcd

Samba

A remotely exploitable stack buffer overflow exists in the Samba server daemon. Versions 2.2.2 through 2.2.6 of Samba contain a remotely exploitable stack buffer overflow.

The Samba Team describes the vulnerability as follows: There was a bug in the length checking for encrypted password change requests from clients. A client could send an encrypted password, which, when decrypted with the old hashed password could be used as a buffer overrun attack on the stack of smbd.

The attach would have to be crafted such that converting a DOS codepage string to little endian UCS2 unicode would translate into an executable block of code. A remote attacker can execute arbitrary code with superuser privileges or can cause smbd to crash.

CERT reference VU#958321

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.

cups

iDefense reported several security problems in CUPS that can lead to local and remote root compromise. An integer overflow in the HTTP interface can be used to gain remote access with CUPS privilege. A local file race condition can be used to gain root privilege, although the previous bug must be exploited first. An attacker can remotely add printers to the vulnerable system.

A remote DoS attack can be accomplished due to negative length in the memcpy() call. An integer overflow in image handling code can be used to gain higher privilege. An attacker can gain local root privilege due to a buffer overflow of the 'options' buffer. A design problem can be exploited to gain local root access, however this needs an added printer (which can also be done, as per a previously noted bug).

Wrong handling of zero-width images can be abused to gain higher privilege. Finally, a file descriptor leak and DoS due to missing checks of return values of file/socket operations.

Mandrake reference MDKSA-2003:001: cups

wget

A vulnerability in all versions of wget prior to and including 1.8.2 was discovered by Steven M. Christey.

The bug permits a malicious FTP server to create or overwrite files anywhere on the local file system by sending filenames beginning with "/" or containing "/../". This can be used to make vulnerable FTP clients write files that can later be used for attack against the client machine.

Mandrake reference MDKSA-2002:086: wget

krb5

A stack buffer overflow in the implementation of the Kerberos v4 compatibility administration daemon (kadmind4) in the krb5 package can be exploited to gain unauthorized root access to a KDC host.

Authentication to the daemon is not required to successfully perform the attack and according to MIT at least one exploit is known to exist. kadmind4 is used only by sites that require compatibility with legacy administrative clients, and sites that do not have these needs are not likely to be using kadmind4 and are not affected.

Mandrake reference MDKSA-2002:073-1: krb5

MySQL

Two vulnerabilities were discovered in all versions of MySQL prior to 3.23.53a and 4.0.5a by Stefan Esser. The first can be used by any valid MySQL user to crash the MySQL server, the other allows anyone to bypass the MySQL password check or execute arbitrary code with the privilege of the user running mysqld.

Another two vulnerabilities were found, one an arbitrary size heap overflow in the mysql client library and another that allows one to write.

Mandrake reference MDKSA-2002:087: MySQL

Fetchmail

Updated Fetchmail packages are available for Red Hat Linux versions 6.2, 7, 7.1, 7.2, 7.3, and 8.0 which close a remotely-exploitable vulnerability in unaltered versions of Fetchmail prior to 6.2.0.

A bug in the header parsing code allows a remote attacker to crash Fetchmail and potentially execute arbitrary code by sending a carefully crafted email which is then parsed by Fetchmail. All users of Fetchmail are advised to upgrade to the errata packages containing a back-ported fix which corrects this issue.

Red Hat reference RHSA-2002:293-09

Canna

The Canna server, used for Japanese character input, has two security vulnerabilities including an exploitable buffer overrun allowing a local user to gain 'bin' user privileges.

Canna is a kana-kanji conversion server which is necessary for Japanese language character input.A buffer overflow bug in the Canna server up to and including version 3.5b2 allows a local user to gain the privileges of the user 'bin' which could lead to further exploits. Updated packages for Red Hat Linux are available.

The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2002-1158 to this issue. A lack in the validation of requests has been found that affects Canna version 3.6 and earlier. A malicious remote user could exploit this vulnerability to leak information, or cause a denial of service attack. (CAN-2002-1159)

Red Hat Linux 7.1, 7.2, 7.3, and 8.0 ship with a Canna package vulnerable to these issues; however, the package is normally only installed when Japanese language support is selected during installation.

All users of Canna are advised to upgrade to these errata packages which contain a back-ported security fix and are not vulnerable to this issue. Red Hat would like to thank hsj and AIDA Shinra for the responsible disclosure of these issues.

Red Hat reference RHSA-2002:246-18

cyrus imapd

The cyrus imapd contains a buffer overflow which could be exploited by remote attackers prior to logging in. Attackers could generate oversized error messages and overflow buffers inside imapd. Additionally to this fix, an overflow in the SASL library (as used by the cyrus imapd) has been fixed.

This bug only affects SuSE Linux 8.1, the SuSE Linux Enterprise Server 8 and the SuSE Linux Openexchange Server. Since there is no workaround possible except shutting down the IMAP server, SuSE strongly recommends an update. Please download the update package for your distribution and verify its integrity. The SuSE website will have more details on how best to do this. Once done, install the package using the command "rpm -Fhv file.rpm" to apply the update.

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

```
/etc/rc.d/cyrus restart
```

and (if using saslauthd)

```
/etc/rc.d/saslauthd restart
```

SuSE reference SuSE-SA:2002:048