Insecurity News

CUPS

The Common UNIX Printing System (CUPS) is a print service. Alvaro Martinez Echevarria reported a bug in the CUPS Internet Printing Protocol (IPP) implementation in versions of CUPS prior to 1.1.21. An attacker could send a carefully crafted UDP packet to the IPP port, which could cause CUPS to stop listening to the port and result in a denial of service. In order to exploit this bug, an attacker would need to have the ability to send a UDP packet to the IPP port (by default 631). The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0558 to this issue.

Debian reference: DSA-545-1
Gentoo reference: GLSA 200410-06 / cups
Mandrake reference: MDKSA-2004:097
Red Hat reference: RHSA-2004:449-17
Slackware reference: SSA:2004-266-01
Suse reference: SUSE-SA:2004:031

getmail

getmail is a reliable fetchmail replacement that supports Maildir, Mboxrd and external MDA delivery.

David Watson discovered a vulnerability in getmail when it is configured to run as root and deliver mail to the maildirs/mbox files of untrusted local users. A malicious local user can then exploit a race condition, or a similar symlink attack, and potentially cause getmail to create or overwrite files in any directory on the system.

Do not run getmail as a privileged user; or, in version 4, use an external MDA with eplicitly configured user and group privileges. All getmail users should upgrade to the latest version:

Debian reference: DSA-553-1
Gentoo reference: GLSA 200409-32 / getmail
Slackware reference: SSA:2004-278-01

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.

Mozilla

Mozilla is an open source Web browser, advanced email and newsgroup client, IRC chat client, and HTML editor. Several recent

Jesse Ruderman discovered a cross-domain scripting bug in Mozilla. If a user is tricked into dragging a Javascript link into another frame or page, it becomes possible for an attacker to steal or modify sensitive information from that site. Additionally, if a user is tricked into dragging two links in sequence to another window (not frame), it is possible for the attacker to execute arbitrary commands. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0905 to this issue.

Gael Delalleau discovered an integer overflow that affects the BMP handling code inside Mozilla. An attacker could create a carefully crafted BMP file in such a way that it would cause Mozilla to crash or execute arbitrary code when the image was viewed. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0904 to this issue.

Georgi Guninski discovered a stack-based buffer overflow in the vCard display routines. An attacker could create a carefully crafted vCard file in such a way that it would cause Mozilla to crash or execute arbitrary code when viewed. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0903 to this issue.

Wladimir Palant discovered a flaw in the way Javascript interacts with the clipboard. It is possible for an attacker to use malicious Javascript code to steal sensitive data which has been copied into the clipboard. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0908 to this issue.

Georgi Guninski discovered a heap-based buffer overflow in the "Send Page" feature. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0902 to this issue.

Red Hat reference: RHSA-2004:486-18
Slackware reference: SSA:2004-266-03
Suse reference: SUSE-SA:2004:036

gtk+

The gtk2 package contains the GIMP ToolKit (GTK+), a library for creating graphical user interfaces for the X Window System.

During testing of a previously fixed flaw in Qt (CAN-2004-0691), a flaw was discovered in the BMP image processor of gtk2. An attacker could create a carefully crafted BMP file which would cause an application to enter an infinite loop and not respond to user input when the file was opened by a victim. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0753 to this issue.

During a security audit Chris Evans discovered a stack and a heap overflow in the XPM image decoder. An attacker could create a carefully crafted XPM file which could cause an application linked with gtk2 to crash or possibly execute arbitrary code when the file was opened by a victim. (CAN-2004-0782, CAN-2004-0783)

Chris Evans also discovered an integer overflow in the ICO image decoder.

An attacker could create a carefully crafted ICO file which could cause an application linked with gtk2 to crash when the file was opened by a victim. (CAN-2004-0788)

Debian reference: DSA-549-1
Red Hat reference: RHSA-2004:466-12
Slackware reference: SSA:2004-266-02
Suse reference: SUSE-SA:2004:033

webmin

webmin is a web-based administration toolkit. Ludwig Nussel discovered a problem when a temporary directory is used but without checking for the previous owner.

Debian reference: DSA-544-1
Mandrake reference: MDKSA-2004:101

OpenOffice.org

OpenOffice.org is an office productivity suite that includes desktop applications such as a word processor, spreadsheet, presentation manager, formula editor, and drawing program.

Secunia Research reported an issue with the handling of temporary files in OpenOffice.org. A malicious local user could use this flaw to access the contents of another user's open documents. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0752 to this issue.

All users of OpenOffice.org are advised to upgrade to the updated OpenOffice.org packages, which contain a backported patch to correct this issue.

Mandrake reference: MDKSA-2004:103
Red Hat reference: RHSA-2004:446-08

SpamAssassin

SpamAssassin provides a way to reduce unsolicited commercial email (SPAM) from incoming email.

A denial of service bug has been found in SpamAssassin versions below 2.64. A malicious attacker could construct a message in such a way that would cause SpamAssassin to stop responding. This denial of service attack would potentially preventing the delivery or filtering of email. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0796 to this issue.

Users of SpamAssassin should update their systems to include the update package that addresses this problem. The updated package contains a backported patch that is not vulnerable to this denial of service attack.

Red Hat reference: RHSA-2004:451-05

XFree86

XFree86 is an open source implementation of the X Window System. It provides the basic low-level functionality that full fledged graphical user interfaces (GUIs) such as GNOME and KDE are designed upon.

During a source code audit, Chris Evans discovered several stack overflow flaws and an integer overflow flaw in the X.Org *libXpm* library used to decode XPM (X PixMap) images. An attacker who knows about this problem could create a carefully crafted XPM file that would cause an application to crash or potentially execute arbitrary code if the file was opened by a victim. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CAN-2004-0687, CAN-2004-0688, and CAN-2004-0692 to these XFree86 security issues.

A flaw was found in the X Display Manager (XDM). XDM opened a *chooserFd* TCP socket even if the *DisplayManager.requestPort* parameter was set to 0. The effect of this situation is that it allows authorized users to access a computer remotely via X, even if the administrator of the computer has configured XDM to refuse a connection to the computer. Although XFree86 4.3.0 was not vulnerable to this issue, Red Hat Enterprise Linux 3 contained a backported patch which introduced this flaw. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0419 to this issue.

Debian reference: DSA-561-1
Gentoo reference: GLSA 200409-34 / X
Mandrake reference: MDKSA-2004:099
Red Hat reference: RHSA-2004:478-13
Suse reference: SUSE-SA:2004:034