Insecurity News

l2tpd

l2tpd is a GPL implementation of the Layer 2 Tunneling Protocol.

Thomas Walpuski reported a buffer overflow in l2tpd, whereby a remote attacker could potentially cause arbitrary code to be executed by transmitting a specially crafted packet.

In order to exploit the vulnerable code, an attacker would need to fake the establishment of an L2TP tunnel. A remote attacker may then be able to execute arbitrary code with the privileges of the user running l2tpd. It is not known whether this bug is exploitable or remains just theoretical.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0649 to this issue.

Debian reference DSA-530-1 l2tpd -- buffer overflow

Gentoo reference GLSA 200407-17 / net-dialup/l2tpd

netkit-telnet-ssl

b0f discovered a format string error in netkit-telnet-ssl which could theoretically allow a remote attacker to cause the execution of arbitrary code with the privileges of the telnet daemon (the 'telnetd' user by default).

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0640 to this issue.

Debian reference DSA-529-1 netkit-telnet-ssl -- format string

OpenOffice.org

The OpenOffice.org office suite contains an internal libneon library which allows it to connect to WebDAV servers. This internal library is subject to the same vulnerabilities that were fixed in libneon recently. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0398 to this issue.

Mandrake reference MDKSA-2004:078

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.

wv

iDefense discovered a buffer overflow vulnerability in the wv package which could allow an attacker to execute arbitrary code with the privileges of the user running the vulnerable application.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0645 to this issue.

Mandrake reference MDKSA-2004:077

Gentoo reference GLSA 200407-11 / app-text/wv

ipsec-tools

IPSEC uses strong cryptography to provide both authentication and encryption services. A vulnerability in racoon prior to version 20040408a would allow a remote attacker to cause a DoS (memory consumption) via an ISAKMP packet with a large length field.

Another vulnerability in racoon was discovered where, when using RSA signatures, racoon would validate the X.509 certificate but would not validate the signature. This can be exploited by an attacker sending a valid and trusted X.509 certificate and any private key. Using this, they could perform a man-in-the-middle attack and initiate an unauthorized connection.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0607 to this issue.

Mandrake reference MDKSA-2004:069

Red Hat reference RHSA-2004:308-06

GNOME VFS

GNOME VFS is the GNOME virtual file system. It provides a modular architecture and ships with several modules that implement support for file systems, HTTP, FTP, and others. The extfs backends make it possible to implement file systems for GNOME VFS using scripts.

Vulnerabilities have been found in several of the GNOME VFS extfs backend scripts.

An attacker who is able to influence a user to open a specially-crafted URI using gnome-vfs could perform actions as that user. The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0494 to this issue.

Red Hat reference RHSA-2004:373-13

Samba

Samba provides file and printer sharing services to SMB/CIFS clients.

Evgeny Demidov discovered a flaw in the internal routine used by the Samba Web Administration Tool (SWAT) in Samba versions 3.0.2 through 3.0.4.

When decoding base-64 data during HTTP basic authentication, an invalid base-64 character could cause a buffer overflow. This same code is also used to internally decode the sambaMungedDial attribute value when using the ldapsam passdb backend, and to decode input given to the ntlm_auth tool. This buffer overflow can possibly be exploited remotely before any authentication took place to execute arbitrary code.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0600 to this issue.

The Samba team also discovered a buffer overflow in the code used to support the 'mangling method = hash' smb.conf option. You should note that the default setting for this parameter in most vendor distributions is 'mangling method = hash2' and therefore not vulnerable.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0686 to this issue. ■

Suse reference SUSE-SA:2004:022
Mandrake reference MDKSA-2004:071
Red Hat reference RHSA-2004:259-23
Gentoo reference GLSA 200407-21 / Samba

php4/mod php4

PHP is a well known, widely-used HTML-embedded scripting language often used within web server setups.

Stefan Esser found a problem with the "memory_limit" handling of PHP which allows remote attackers to execute arbitrary code as the user running the PHP interpreter. If a remote attacker could force the PHP interpreter to allocate more memory than the memory_limit setting before script execution begins, then the attacker may be able to supply the contents of a PHP hash table remotely. This hash table could then be used to execute arbitrary code as the 'apache' user.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0594 to this issue.

Stefan Esser also discovered a flaw in the strip_tags function in versions of PHP before 4.3.8. The strip_tags function is commonly used by PHP scripts to prevent Cross-Site-Scripting attacks by removing HTML tags from user-supplied form data. By embedding NUL bytes into form data, HTML tags can in some cases be passed intact through the strip_tags function, which may allow a Cross-Site-Scripting attack.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2004-0595 to this issue. ■

Suse reference SUSE-SA:2004:021
Mandrake reference MDKSA-2004:068
Red Hat reference RHSA-2004:392-13
Debian reference DSA-531-1 php4 -- several vulnerabilities
Gentoo reference GLSA 200407-13 / PHP