Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
AhnLab AhnLab V3 prior to 6.0.0.457	Multiple vulnerabilities have been reported in AhnLab V3 that could let local malicious users obtain elevated privileges, obtain arbitrary file access, or execute arbitrary code.	AhnLab V3 DeviceIoControl Multiple Vulnerabilities CAN-2005-3030	High	Security Tracker, Alert ID: 1014908, September 15, 2005

	Upgrade to version 6.0.0.457: http://info.ahnlab.com/english/advisory/01.html Currently we are not aware of any exploits for this vulnerability.	CAN-2005-3029 CAN-2005-3028		
Cambridge Computer Corporation vxFtpSrv 0.9.7	A buffer overflow vulnerability has been reported in vxFtpSrv that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	vxFtpSrv Arbitrary Code Execution CAN-2005-3031	High	Security Tracker, Alert ID: 1014911, September 15, 2005
Cambridge Computer Corporation vxTftpSrv 1.7.0	A buffer overflow vulnerability has been reported in vxTftpSrv that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	vxTftpSrv Arbitrary Code Execution CAN-2005-3032	High	Security Tracker, Alert ID: 1014912, September 15, 2005
Cambridge Computer Corporation vxWeb 1.1.4	A vulnerability has been reported in vxWeb that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	vxWeb Denial of Service CAN-2005-3033	Low	Security Tracker, Alert ID: 1014910, September 15, 2005
Compuware DriverStudio 2.7 and 3.0 beta 2	Multiple vulnerabilities have been reported in DriverStudio that could let local malicious users obtain elevated privileges or execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Compuware DriverStudio Privilege Elevation or Arbitrary Code Execution CAN-2005-3034 CAN-2005-3035	Medium	Security Focus, ID: 14838, 14837, September 15, 2005
Digger Solutions Intranet Open Source 2.7.2	A vulnerability has been reported in Intranet Open Source that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	Digger Solutions Intranet Open Source SQL Injection	Medium	Security Focus, ID: 14882, September 20, 2005
File Transfer Anywhere 3.01	A vulnerability has been reported in File Transfer Anywhere that could let local malicious users disclose password information. A vendor fix is available, contact the vendor. There is no exploit code required.	File Transfer Anywhere Passwords Disclosure CAN-2005-3036	Medium	Security Tracker, Alert ID: 1014919, September 16, 2005
Handy Address Book Handy Address Book Server 1.1	An input validation vulnerability has been reported in Handy Address Book Server that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Handy Address Book Server Cross-Site Scripting CAN-2005-3037	Medium	Security Tracker, Alert ID: 1014901, September 15, 2005
Hosting Controller 6.1 with HF2.3	A vulnerability has been reported in Hosting Controller that could let remote malicious users disclose information. A vendor hotfix (2.4) is available: http://hostingcontroller.com/english/logs/hotfixlogv61_2_4.html Currently we are not aware of any exploits for this vulnerability.	Hosting Controller Information Disclosure CAN-2005-3038	Medium	Secunia, Advisory: SA16824, September 15, 2005
IBM Clearquest 2003.06.15, 2003.06.14, 2003.06.13, 2003.06.12, 2003.06.10, 2003.06.00, 2002.05.20, 2002.05.00	Cross-Site Scripting vulnerabilities have been in XML Style Sheets due to insufficient sanitization of certain parameters, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www-1.ibm.com/support/docview.wss?uid=swg24010127&rs=0&cs=utf-8 &context=SSSH5A&dc=D400&loc=en_US〈=en&cc=US There is no exploit code required.	IBM Rational ClearQuest Multiple Cross-Site Scripting CAN-2005-2994	Medium	IBM Security Advisory, September 20, 2005

Mall23 Mall23 eCommerce	An input validation vulnerability has been reported Mall23 eCommerce ('infopage.asp') that could let remote malicious users perform SQL injection. **A vendor patch is available, contact the vendor.** There is no exploit code required; however, a Proof of Concept exploit script has been published.	Mall23 SQL Injection CAN-2005-3039	Medium	Security Tracker, Alert ID: 1014882, September 12, 2005 **Security Focus, ID: 14803, September 19, 2005**
Sybari Antigen for Exchange 8.0 SR2	A vulnerability has been reported in Antigen for SMTP/ Exchange that could let remote malicious users bypass security restrictions. A vendor update is available: http://www.sybari.com/portal/alias__Rainbow/lang__en-US/tabID__3359/DesktopDefault.aspx There is no exploit code required.	Sybari Antigen for Exchange Security Bypass CAN-2005-3027	Medium	Security Tracker, Alert ID: 1014934, September 19, 2005
TAC Vista 4.0	An input validation vulnerability has been reported in Vista that could let remote malicious users traverse directories. Upgrade to version 4.3: There is no exploit code required; however, a Proof of Concept exploit script has been published.	TAC Vista Directory Traversal CAN-2005-3040	Medium	Security Tracker, Alert ID: 1014923, September 16, 2005
VERITAS Storage Exec 5.3 rev2190R StorageCentral 5.2 rev322	A buffer overflow vulnerability has been reported in Storage Exec/ StorageCentral that could let remote malicious users execute arbitrary code. A vendor fix is available: http://support.veritas.com/docs/277566 Currently we are not aware of any exploits for this vulnerability.	Storage Exec/ StorageCentral Arbitrary Code Execution CAN-2005-2996	High	Secunia Advisory: SA16871, September 20, 2005
Xclusive-software Multi-Computer Control System 1.1	A vulnerability has been reported in Multi-Computer Control System that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Multi-Computer Control System Denial of Service CAN-2005-3002	Low	Secunia, Advisory: SA16865, September 19, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apache Software Foundation Apache 2.0.x	A vulnerability has been reported in 'modules/ssl/ssl_engine_kernel.c' because the 'ssl_hook_Access()' function does not properly enforce the 'SSLVerifyClient require' directive in a per-location context if a virtual host is configured with the 'SSLVerifyCLient optional' directive, which could let a remote malicious user bypass security policies. Patch available at: http://svn.apache.org/viewcvs?rev=264800&view=rev OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/	Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass CAN-2005-2700	Medium	Security Tracker Alert ID: 1014833, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.017, September 3, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 Slackware Security Advisory,

	Debian: http://security.debian.org/pool/updates/main/a/apache2/ Mandriva: http://www.mandriva.com/security/advisories Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/liba/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-12.xml** There is no exploit code required.			SSA:2005-251-02, September 9, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 Debian Security Advisory DSA 807-1, September 12, 2005 US-CERT VU#744929 **Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005**
Apple Safari 2.0.1, 2.0, 1.3, 1.2-1.2.3, 1.0, 1.1	A vulnerability has been reported when the browser opens specific 'data:' URLs, which could lead to a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Apple Safari Data URI Memory Corruption CAN-2005-3018	Low	Security Focus, Bugtraq ID: 14868, September 17, 2005
ARC ARC 5.21 j	A vulnerability was reported due to the insecure creation of temporary new archives by 'arc' and 'marc' before renamed to the user specified filename, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Arc Insecure Temporary File Creation CAN-2005-2945	Medium	Secunia Advisory: SA16805, September 16, 2005
Bacula Bacula 1.36 .3	Vulnerabilities have been reported in 'autoconf/randpass' and 'scripts/mtx-changer.in' due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files. The vulnerabilities have been fixed in the CVS repositories. There is no exploit code required.	Bacula Insecure Temporary File Creation CAN-2005-2995	Medium	Secunia Advisory: SA16866, September 20, 2005
Clam Anti-Virus ClamAV 0.80 -0.86.2, 0.70, 0.65-0.68, 0.60, 0.51-0.54	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'libclamav/upx.c' due to a signedness error, which could let a malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported in 'libclamav/fsg.c' when handling a specially -crafted FSG-compressed executable file. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=86638 Gentoo: http://security.gentoo.org/glsa/glsa-200509-13.xml Currently we are not aware of any exploits for these vulnerabilities.	ClamAV UPX Buffer Overflow & FSG Handling Denial of Service CAN-2005-2919 CAN-2005-2920	High	Secunia Advisory: SA16848, September 19, 2005 Gentoo Linux Security Advisory, GLSA 200509-13, September 19, 2005
Easy Software Products CUPS prior to 1.1.21rc1	A vulnerability has been reported in incoming print jobs due to a failure to properly apply ACLs (Access Control List), which could let a remote malicious user bypass ACLs. Upgrades available at: http://www.cups.org/software.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-571.html **Fedora:** **http://download.fedoralegacy.org/fedora/**	Easy Software Products CUPS Access Control List Bypass CAN-2004-2154	Medium	Security Tracker Alert ID: 1014482, July 14, 2005 RedHat Security Advisory, RHSA-2005: 571-06, July 14, 2005 **Fedora Legacy Update Advisory, FLSA:163274, September 14, 2005** **Ubuntu Security Notice,**

	Ubuntu: **http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/** There is no exploit code required.			**USN-185-1, September 20, 2005**
Gnome Development Team Gnome Workstation Command Center 0.9.8	A vulnerability has been reported due to the insecure creation of the 'gwcc_out.txt' temporary file, which could let a malicious user create/overwrite arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	GNOME Workstation Command Center Insecure Temporary File Creation CAN-2005-2944	Medium	Security Focus, Bugtraq ID: 14857, September 16, 2005
GNU Mailutils 0.6	A format string vulnerability has been reported in 'search.c' when processing user-supplied IMAP SEARCH commands, which could let a remote malicious user execute arbitrary code. Patch available at: http://savannah.gnu.org/patch/download.php?item_id=4407&item_file_id=5 160 **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-10.xml** A Proof of Concept exploit script has been published.	GNU Mailutils Format String CAN-2005-2878	High	Security Tracker Alert ID: 1014879, September 9, 2005 **Gentoo Linux Security Advisory, GLSA 200509-10, September 17, 2005**
GNU Texinfo 4.7	A vulnerability has been reported in 'textindex.c' due to insecure creation of temporary files by the 'sort_offline()' function, which could let a malicious user create/overwrite arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	GNU Texinfo Insecure Temporary File Creation CAN-2005-3011	Medium	Security Focus, Bugtraq ID: 14854, September 15, 2005
Grip Grip 3.1.2, 3.2 .0	A buffer overflow vulnerability has been reported in the CDDB protocol due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200503-21.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-304.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200504-07.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** Currently we are not aware of any exploits for this vulnerability.	Grip CDDB Query Buffer Overflow CAN-2005-0706	High	Fedora Update Notifications, FEDORA-2005-202 & 203, March 9, 2005 Gentoo Linux Security Advisory, GLSA 200503-21, March 17, 2005 RedHat Security Advisory, RHSA-2005:304-08, March 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:066, April 3, 2005 Gentoo Linux Security Advisory, GLSA 200504-07, April 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:010, April 8, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:074 & 075, April 21, 2005 Peachtree Linux Security Notice, PLSN-0007, April 22, 2005 **Fedora Legacy Update Advisory, FLSA:152919, September 15, 2005**

GtkDiskFree GtkDiskFree 1.9.3	A vulnerability has been reported in the 'src/mount.c' file due to the insecure creation of temporary files, which could let a malicious user cause a Denial of Service or overwrite files. No workaround or patch available at time of publishing. There is no exploit code required.	GTKDiskFree Insecure Temporary File Creation CAN-2005-2918	Medium	ZATAZ Audits Advisory, September 15, 2005
Hewlett Packard Company Tru64 5.1 B-3, 5.1 B-2 PK4, 5.1 A PK, 4.0 G PK4, 4.0 F PK8	A remote Denial of Service vulnerability has been reported caused due to an unspecified error in the FTP daemon. Upgrades available at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBTU01227 Currently we are not aware of any exploits for this vulnerability.	HP Tru64 FTP Server Remote Denial of Service CAN-2005-2993	Low	HP Security Bulletin, HPSBTU01227, September 20, 2005
LibTIFF LibTIFF 3.4, 3.5.1-3.5.5, 3.5.7, 3.6.0, 3.6.1, 3.7, 3.7.1	A buffer overflow vulnerability has been reported in the 'TIFFOpen()' function when opening malformed TIFF files, which could let a remote malicious user execute arbitrary code. Patches available at: http://bugzilla.remotesensing.org/attachment.cgi?id=238 Gentoo: http://security.gentoo.org/glsa/glsa-200505-07.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tiff/ SuSE: ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Debian: http://security.debian.org/pool/updates/main/t/tiff/ **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.34** Currently we are not aware of any exploits for this vulnerability.	LibTIFF TIFFOpen Remote Buffer Overflow CAN-2005-1544 CAN-2005-1472	High	Gentoo Linux Security Advisory, GLSA 200505-07, May 10, 2005 Ubuntu Security Notice, USN-130-1, May 19, 2005 SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005 Turbolinux Security Advisory, TLSA-2005-72, June 28, 2005 Debian Security Advisory, DSA 755-1, July 13, 2005 **SCO Security Advisory, SCOSA-2005.34, September 19, 2005**
LineControl LineContol Java Client 0.8	A vulnerability has been reported in 'AuthInfo.java' due to an error, which could let a malicious user obtain password information. Upgrade available at: http://prdownloads.sourceforge.net/linecontrol/jlc-0.8.1.tar.gz There is no exploit code required.	LineControl Java Client Password Disclosure CAN-2005-2990	Medium	Secunia Advisory: SA16817, September 14, 2005

lm_sensors lm_sensors 2.9.1	A vulnerability has been reported in the 'pwmconfig' script due to the insecure creation of temporary files, which could result in a loss of data or a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lm-sensors/ Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200508-19.xml **Debian:** **http://security.debian.org/pool/updates/main/l/lm-sensors/** There is no exploit code required.	LM_sensors PWMConfig Insecure Temporary File Creation CAN-2005-2672	Low	Security Focus, Bugtraq ID: 14624, August 22, 2005 Ubuntu Security Notice, USN-172-1, August 23, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:149, August 25, 2005 Gentoo Linux Security Advisory, GLSA 200508-19, August 30, 2005 **Debian Security Advisory, DSA 814-1, September 15, 2005**
MasqMail MasqMail 0.2.18	Several vulnerabilities have been reported: a vulnerability was reported in the email address due to a sanitization error when the message fails to be sent, which could let a malicious user execute arbitrary commands with privileges of the mail user; and a vulnerability was reported when handling log files due to an unspecified error, which could let a remote malicious user overwrite arbitrary files. Mandriva: http://www.mandriva.com/security/advisories There is no exploit code required.	MasqMail Elevated Privileges CAN-2005-2662 CAN-2005-2663	Medium	Mandriva Linux Security Update Advisory, MDKSA-2005:168, September 20, 2005

Multiple Vendors
Glyph and Cog Xpdf 3.0, pl2 & pl3;
Ubuntu Linux 5.0 4 powerpc, i386, amd64;
RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0;
KDE 3.4.1, 3.4, 3.3.1, 3.3.2;
GNOME GPdf 2.8.3, 2.1
	A remote Denial of Service vulnerability has been reported when verifying malformed 'loca' table in PDF files.
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-670.html
	http://rhn.redhat.com/errata/RHSA-2005-671.html
	http://rhn.redhat.com/errata/RHSA-2005-708.html
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/x/xpdf/
	KDE:
	http://www.kde.org/info/security/advisory-20050809-1.txt
	Mandriva:
	http://www.mandriva.com/security/advisories
	SGI:
	ftp://patches.sgi.com/support/free/security/advisories/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200508-08.xml
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Debian:
	http://security.debian.org/pool/updates/main/k/kdegraphics/
		XPDF Loca Table Verification Remote Denial of Service
		CAN-2005-2097
			Low	RedHat Security Advisories, RHSA-2005:670-05 & RHSA-2005:671-03, & RHSA-2005:708-05, August 9, 2005
				Ubuntu Security Notice, USN-163-1, August 09, 2005
				KDE Security Advisory, 20050809-1, August 9, 2005
				Mandriva Linux Security Update Advisories, MDKSA-2005:134, 135, 136 & 138, August 11, 2005
				SGI Security Advisory, 20050802-01-U, August 15, 2005
				Gentoo Linux Security Advisory GLSA, 200508-08, August 16, 2005
				Fedora Update Notifications, FEDORA-2005-729, 730, 732, & 733, August 15 & 17, 2005
				Debian Security Advisory, DSA 780-1, August 22, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005
				Turbolinux Security Advisory, TLSA-2005-88, September 5, 2005
				Conectiva Linux Announce-ment, CLSA-2005:1010,

	Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.			September 13, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:138-1, September 19, 2005**
Multiple Vendors Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6	A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges. A fixed version (5.8.4 or later) is available at: http://www.perl.com/CPAN/src/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml Debian: http://security.debian.org/pool/updates/main/p/perl/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Mandrake: http://www.mandrakesecure.net/en/ftp.php HP: http://software.hp.com/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-196.pdf** Currently we are not aware of any exploits for this vulnerability.	Perl 'rmtree()' Function Elevated Privileges CAN-2005-0448	Medium	Ubuntu Security Notice, USN-94-1 March 09, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 Debian Security Advisory, DSA 696-1 , March 22, 2005 Turbolinux Security Advisory, TLSA-2005-45, April 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:079, April 29, 2005 HP Security Bulletin, HPSBUX01208, June 16, 2005 Secunia, Advisory: SA16193, July 25, 2005 **Avaya Security Advisory, ASA-2005-196, September 13, 2005**
Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3 , 0.1-0.1.6 1, 0.0.1-0.0.6	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.suse.com/pub/suse/ Ubuntu:	Zlib Compression Library Buffer Overflow CAN-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005

	http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/security/advisories OpenBSD: http://www.openbsd.org/errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ zsync: http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download Apple: http://docs.info.apple.com/article.html?artnum=302163 SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id = 35093&release_id=351848 Debian: http://security.debian.org/pool/updates/main/z/zsync/ Trolltech: ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** Currently we are not aware of any exploits for this vulnerability.		Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Security Focus, Bugtraq ID: 14162, August 26, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14162, September 12, 2005 **Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005**

Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib: http://www.zlib.net/zlib-1.2.3.tar.gz Debian: http://security.debian.org/pool/updates/main/z/zlib/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ OpenBSD: http://www.openbsd.org/errata.html#libz2 Mandriva: http://www.mandriva.com/security/ advisories?name=MDKSA-2005:124 Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.323596 FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc SUSE: http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html Gentoo: http://security.gentoo.org/glsa/glsa-200507-28.xml http://security.gentoo.org/glsa/glsa-200508-01.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Apple: http://docs.info.apple.com/article.html?artnum=302163 TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 Debian: http://security.debian.org/pool/updates/main/z/zsync/ Trolltech:	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CAN-2005-1849	Low	Security Focus, Bugtraq ID 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005 FreeBSD Security Advisory, SA-05:18, July 27, 2005 SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005 Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005 Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005 Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005 Turbolinux Security Advisory , TLSA-2005-83, August 18, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14340, September 12, 2005 **Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005**

ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz

FedoraLegacy:
http://download.fedoralegacy.org/fedora/

Currently we are not aware of any exploits for this vulnerability.

Multiple Vendors
 	
Gentoo Linux;
RedHat Fedora Core3, Core2;
SUSE Linux 8.1, 8.2, 9.0-9.2, Desktop 1.0, Enterprise Server 9, 8,
Novell Linux Desktop 1.0;
X.org X11R6 6.7 .0, 6.8, 6.8.1;
XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0-4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1
4.3 .0
	Multiple vulnerabilities have been reported due to integer overflows, memory access errors, input validation errors, and logic errors, which could let a remote malicious user execute arbitrary code, obtain sensitive information, or cause a Denial of Service.
	
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates
	
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200411-28.xml
	
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	
	X.org:
	http://www.x.org/pub/
	
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
	
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2004-537.html
	
	Mandrakesoft:
	http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:137
	(libxpm)
	
	http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:138
	(XFree86)
	
	Debian:
	http://www.debian.org/security/2004/dsa-607
	(XFree86)
	
	SGI:
	ftp://patches.sgi.com/support/free/security/patches/ProPack/3/
	
	TurboLinux:
	http://www.turbolinux.com/update/
	
	Avaya:
	http://support.avaya.com/elmodocs2/security/ASA-2005-023_RHSA-2004-537.pdf
	
	http://support.avaya.com/|elmodocs2/security/ASA-2005-025_RHSA-2005-004.pdf
	
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200502-06.xml
	
	http://security.gentoo.org/glsa/glsa-200502-07.xml
	
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/
	
	FedoraLegacy:
	http://download.fedoralegacy.org/redhat/
	
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/
		Multiple Vendors LibXPM Multiple Vulnerabilities
		
		CAN-2004-0914
			High	X.Org Foundation Security Advisory, November 17, 2004
				
				Fedora Update Notifications,
				FEDORA-2004-433 & 434, November 17 & 18, 2004
				
				SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004
				
				Gentoo Linux Security Advisory, GLSA 200411-28, November 19, 2004
				
				Fedora Security Update Notifications
				FEDORA-2003-464, 465, 466, & 467, December 1, 2004
				
				RedHat Security Advisory, RHSA-2004:537-17, December 2, 2004
				
				Mandrakesoft:
				MDKSA-2004:137: libxpm4;
				MDKSA-2004:138: XFree86, November 22, 2004
				
				Debian Security Advisory DSA-607-1 xfree86 -- several vulnerabilities, December 10, 2004
				
				Turbolinux Security Announcement, January 20, 2005
				
				Avaya Security Advisories, ASA-2005-023 & 025, January 25, 2005
				
				Gentoo Linux Security Advisories, GLSA 200502-06 & 07, February 7, 2005
				
				Ubuntu Security Notice, USN-83-1 February 16, 2005
				
				Fedora Legacy Update Advisory, FLSA:2314, March 2, 2005
				
				Ubuntu Security Notice, USN-83-2, September 12, 2005
				
				HP Security Bulletin, HPSBTU01228, September 20, 2005

	HP: **http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBTU01228** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Linux kernel 2.6.8-2.6.10, 2.4.21	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'msg_control' when copying 32 bit contents, which could let a malicious user obtain root privileges and execute arbitrary code; and a vulnerability was reported in the 'raw_sendmsg()' function, which could let a malicious user obtain sensitive information or cause a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service CAN-2005-2490 CAN-2005-2492	High	Secunia Advisory: SA16747, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; GNOME Evolution 2.3.1 -2.3.6 .1, 2,0- 2.2 , 1.5	Multiple format string vulnerabilities have been reported: a vulnerability was reported when vCard information is attached to an email message, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when specially crafted contact data that has been retrieved from an LDAP server is displayed, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported when specially crafted task list data that has been retrieved from remote servers and the data has been saved under the 'Calendars' tab is displayed, which could let a remote malicious user execute arbitrary code. Updates available at: http://ftp.gnome.org/pub/gnome/sources/evolution/2.3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-12.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-267.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.	GNOME Evolution Multiple Format String CAN-2005-2549 CAN-2005-2550	High	Secunia Advisory: SA16394, August 11, 2005 Ubuntu Security Notice, USN-166-1, August 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:141, August 18, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 Gentoo Linux Security Advisory, GLSA 200508-12, August 23, 200 RedHat Security Advisory, RHSA-2005:267-10, August 29, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Conectiva Linux Announce-ment, CLSA-2005:1004, September 13, 2005 **SUSE Security Announcement, SUSE-SA:2005:054, September 16, 2005**

Multiple Vendors util-linux 2.8-2.13; Andries Brouwer util-linux 2.11 d, f, h, i, k, l, n, u, 2.10 s	A vulnerability has been reported because mounted filesystem options are improperly cleared due to a design flaw, which could let a remote malicious user obtain elevated privileges. Updates available at: http://www.kernel.org/pub/linux/utils/util-linux/testing/util-linux-2.12r-pre1.tar.gz Slackware: ftp://ftp.slackware.com/pub/slackware/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/u/util-linux/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-15.xml** **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	Util-Linux UMount Remounting Filesystem Elevated Privileges CAN-2005-2876	Medium	Security Focus, Bugtraq ID: 14816, September 12, 2005 Slackware Security Advisory, SSA:2005-255-02, September 13, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005** **Ubuntu Security Notice, USN-184-1, September 19, 2005** **Gentoo Linux Security Advisory, GLSA 200509-15, September 20, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:167, September 20, 2005**

Multiple Vendors
XFree86 X11R6 4.3 .0, 4.1 .0; X.org X11R6 6.8.2;
RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Advanced Workstation for the Itanium Processor 2.1, IA64;
Gentoo Linux
	A buffer overflow vulnerability has been reported in the pixmap processing code, which could let a malicious user execute arbitrary code and possibly obtain superuser privileges.
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200509-07.xml
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-329.html
	http://rhn.redhat.com/errata/RHSA-2005-396.html
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/
	Mandriva:
	http://www.mandriva.com/security/advisories?name=MDKSA-2005:164
	Sun:
	http://sunsolve.sun.com/search/document.do?assetkey=1-26-101926-1&searchclause
	Currently we are not aware of any exploits for this vulnerability.
		XFree86 Pixmap Allocation Buffer Overflow
		CAN-2005-2495
			High	Gentoo Linux Security Advisory, GLSA 200509-07, September 12, 2005
				RedHat Security Advisory, RHSA-2005:329-12 & RHSA-2005:396-9, September 12 & 13, 2005
				Ubuntu Security Notice, USN-182-1, September 12, 2005
				Mandriva Security Advisory, MDKSA-2005:164, September 13, 2005
				US-CERT VU#102441
				Sun(sm) Alert Notification Sun Alert ID: 101926, September 19, 2005

ncompress ncompress 4.2.4	A vulnerability has been reported in the 'build,' 'zcmp,' and 'zdiff' scripts due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges No workaround or patch available at time of publishing. There is no exploit code required.	Ncompress Insecure Temporary File Creation CAN-2005-2991	Medium	Secunia Advisory: SA16827, September 16, 2005
netpbm 10.0	A vulnerability has been reported in netpbm ('-dSAFER') that could let malicious users execute arbitrary postscript code. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-04.xml	netpbm Arbitrary Code Execution CAN-2005-2471	High	Secunia Advisory: SA16184, July 25, 2005 Trustix Secure Linux Security Advisory, #2005-0038, July 29, 2005 Gentoo Linux Security Advisory, GLSA 200508-04, August 5, 2005 Mandriva Linux Security

	Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-743.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.			Update Advisory, MDKSA-2005:133, August 10, 2005 Ubuntu Security Notice, USN-164-1, August 11, 2005 Fedora Update Notifications, FEDORA-2005-727 & 728, August 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 RedHat Security Advisory, RHSA-2005:743-08, August 22, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 **Conectiva Linux Announcement, CLSA-2005:1007, September 13, 2005** **Turbolinux Security Advisory, TLSA-2005-90, September 20, 2005**
PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-17.xml Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Debian: http://security.debian.org/pool/updates/main/p/pcre3/ SUSE: ftp://ftp.SUSE.com/	PCRE Regular Expression Heap Overflow CAN-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices, USN-173-1 & 173-2, August 24, 2005 Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005 SUSE Security Announcements, SUSE-SA:2005:048 & 049, August 30, 2005 Slackware Security Advisories, SSA:2005-242-01 & 242-02 , August 31, 2005 Ubuntu Security Notices, USN-173-3, 173-4 August 30 & 31, 2005 Debian Security Advisory, DSA 800-1, September 2, 2005 SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005

	pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.1/testing/packages/php-5.0.5/php-5.0.5-i486-1.tgz Gentoo: http://security.gentoo.org/glsa/glsa-200509-08.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-12.xml** Currently we are not aware of any exploits for this vulnerability.			Slackware Security Advisory, SSA:2005-251-04, September 9, 2005 Gentoo Linux Security Advisory, GLSA 200509-08, September 12, 2005 Conectiva Linux Announce-ment, CLSA-2005:1009, September 13, 2005 **Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005**
PHP PHP 4.4.0, 4.3-4.3.11, 4.2-4.2.3, 4.1.0-4.1.2, 4.0 0-4.0.7, 3.0 0 -3.0.18	A vulnerability has been reported due to the way session variables are stored, which could let a malicious user hijack sessions variables. No workaround or patch available at time of publishing. There is no exploit code required.	PHP Session Hijacking	Medium	Security Focus, Bugtraq ID: 14858, September 16, 2005
Postgre SQL PostgreSQL 7.3 through 8.0.2	Two vulnerabilities have been reported: a vulnerability was reported because a remote authenticated malicious user can invoke some client-to-server character set conversion functions and supply specially crafted argument values to potentially execute arbitrary commands; and a remote Denial of Service vulnerability was reported because the 'contrib/tsearch2' module incorrectly declares several functions as returning type 'internal.' Fix available at: http://www.postgresql.org/about/news.315 Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-12.xml Trustix: http://www.trustix.org/errata/2005/0023/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-433.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for these vulnerabilities.	PostgreSQL Remote Denial of Service & Arbitrary Code Execution CAN-2005-1409 CAN-2005-1410	High	Security Tracker Alert, 1013868, May 3, 2005 Ubuntu Security Notice, USN-118-1, May 04, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-12, May 16, 2005 Trustix Secure Linux Bugfix Advisory, TSL-2005-0023, May 16, 2005 Turbolinux Security Advisory , TLSA-2005-62, June 1, 2005 RedHat Security Advisory, RHSA-2005:433-17, June 1, 2005 SGI Security Advisory, 20050602-01-U, June 23, 2005 **Conectiva Linux Announcement, CLSA-2005:1008, September 13, 2005**
PostgreSQL PostgreSQL 7.4.5; Avaya CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0	A vulnerability was reported due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/	PostgreSQL Insecure Temporary File Creation CAN-2004-0977	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory, GLSA 200410-16, October 18, 2004 Debian Security Advisory, DSA 577-1, October 29,

	glsa/glsa-200410-16.xml Debian: http://security.debian.org/pool/updates/main/p/postgresql/ OpenPKG: ftp://ftp.openpkg.org/release/ Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:149 Red Hat: http://rhn.redhat.com/errata/RHSA-2004-489.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-024_RHSA-2004-489.pdf **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.			2004 OpenPKG Security Advisory, OpenPKG-SA-2004.046, October 29, 2004 Mandrakesoft Security Advisory, MDKSA-2004:149, December 13, 2004 Red Hat Advisory RHSA-2004:489-17, December 20, 2004 Avaya Security Advisory, ASA-2005-024, January 25, 2005 Turbolinux Security Announcement, February 17, 2005 **Conectiva Linux Announcement, CLSA-2005:1008, September 13, 2005**
Rob Flynn Gaim prior to 1.3.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported when using the Yahoo! protocol to download a file; and a remote Denial of Service vulnerability was reported in the MSN Messenger service when a malicious user submits a specially crafted MSN message. Updates available at: http://gaim.sourceforge.net/downloads.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200506-11.xml Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-518.html Debian: http://security.debian.org/pool/updates/main/g/gaim/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.	Gaim Multiple Remote Denial of Services CAN-2005-1269 CAN-2005-1934	Low	Secunia Advisory, SA15648, June 10, 2005 Ubuntu Security Notice USN-139-1, June 10, 2005 Gentoo Linux Security Advisory, GLSA 200506-11, June 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:099, June 14, 2005 Fedora Update Notifications, FEDORA-2005-410, & 411, June 17, 2005 RedHat Security Advisory, RHSA-2005:518-03, June 16, 2005 Debian Security Advisory, DSA 734-1, July 5, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Debian Security Advisory, DSA 773-1, August 11, 2005 **Conectiva Linux Announcement, CLSA-2005:1006, September 13, 2005**

Shorewall Shorewall 2.0.x, 2.2.x, 2.4.x	A vulnerability has been reported due to a failure to properly implement expected firewall rules for MAC address-based filtering, which could let a remote malicious user bypass firewall rules. Hotfixes available at: http://www.shorewall.net/ Mandriva: http://www.mandriva.com/ security/advisories **Gentoo:** **http://security.gentoo.org/ glsa/glsa-200507-20.xml** There is no exploit code required.	Shorewall MACLIST Firewall Rules Bypass CAN-2005-2317	Medium	Secunia Advisory: SA16087, July 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:123, July 21, 2005 **Gentoo Linux Security Advisory [ERRATA UPDATE], GLSA 200507-20:02, September 17, 2005**
Simple CDR-X SimpleCDR-X 1.3.3	A vulnerability has been reported due to the insecure creation of a temporary copy of the ISO image, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	SimpleCDR-X Insecure Temporary File Creation CAN-2005-3012	Medium	Secunia Advisory: SA16835, September 16, 2005
slocate slocate 2.7	A Denial of Service vulnerability has been reported when a specially crafted directory structure that contains long paths is submitted. Mandriva: http://www.mandriva.com/ security/advisories **TurboLinux:** **ftp://ftp.turbolinux.co.jp/ pub/TurboLinux/ TurboLinux/ia32/** There is no exploit code required.	slocate Long Path Denial of Service CAN-2005-2499	Low	Mandriva Linux Security Update Advisory, MDKSA-2005:147, August 22, 2005 **Turbolinux Security Advisory, TLSA-2005-91, September 20, 2005**
Squid Web Proxy Squid Web Proxy Cache 2.5 & prior	A remote Denial of Service vulnerability has been reported in the 'storeBuffer()' function when handling aborted requests. Patches available at: http://www.squid-cache.org/Versions/ v2/2.5/bugs/squid-2.5.STABLE 10-STORE_PENDING.patch Gentoo: http://security.gentoo.org/ glsa/glsa-200509-06.xml OpenPKG: ftp://ftp.openpkg.org/ release/ Mandriva: http://www.mandriva.com/ security/advisories Debian: http://security.debian.org/ pool/updates/main/ s/squid/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/universe/ s/squid/ **RedHat:** **http://rhn.redhat.com/ errata/RHSA-2005-766.html** **SUSE:** **ftp://ftp.suse.com /pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Squid Aborted Requests Remote Denial of Service CAN-2005-2794	Low	Security Tracker Alert ID: 1014864, September 7, 2005 Gentoo Linux Security Advisory GLSA 200509-06, September 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.021, September 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:162, September 12, 2004 Debian Security Advisory, DSA 809-1, September 13, 2005 Ubuntu Security Notice, USN-183-1, September 13, 2005 **RedHat Security Advisory, RHSA-2005:766-7, September 15, 2005** **SUSE Security Announcement, SUSE-SA:2005:053, September 16, 2005**

Squid Web Proxy Squid Web Proxy Cache 2.5 .STABLE1-STABLE 10, 2.4 .STABLE6 & 7, STABLE 2, 2.4, 2.3 STABLE 4&5, 2.1 Patch 2, 2.0 Patch 2	A remote Denial of Service vulnerability has been reported in '/squid/src/ssl.c' when a malicious user triggers a segmentation fault in the 'sslConnectTimeout()' function. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-sslConnectTimeout.patch Trustix: http://http.trustix.org/pub/trustix/updates/ OpenPKG: ftp://ftp.openpkg.org/release/ Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Debian: http://security.debian.org/pool/updates/main/s/squid/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-766.html** **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	Squid 'sslConnectTimeout()' Remote Denial of Service CAN-2005-2796	Low	Security Tracker Alert ID: 1014846, September 2, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.021, September 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:162, September 12, 2005 Ubuntu Security Notice, USN-183-1, September 13, 2005 Debian Security Advisory, DSA 809-1, September 13, 2005 **RedHat Security Advisory, RHSA-2005:766-7, September 15, 2005** **SUSE Security Announcement, SUSE-SA:2005:053, September 16, 2005**
Sun Microsystems, Inc. Solaris 10.0, _x86	A Denial of Service vulnerability has been reported in the 'ti' driver due to an unspecified error. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101899-1&searchclause Currently we are not aware of any exploits for this vulnerability.	Sun Solaris 'Ti' Driver Denial of Service CAN-2005-3001	Low	Sun(sm) Alert Notification Sun Alert ID: 101899, September 19, 2005
SuSE Linux Professional 9.3 x86_64, 9.3, Linux Personal 9.3 x86_64, 9.3	A buffer overflow vulnerability has been reported in Yast, which could let a malicious user execute arbitrary code with superuser privileges. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	SuSE YaST Buffer Overflow CAN-2005-3013	High	Security Focus, Bugtraq ID: 14861, September 16, 2005
Turquoise SuperStat Turquoise SuperStat 202-2.2.3	A buffer overflow has been reported in the date parser due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://freshmeat.net/redir/turquoise/10809/url_tgz/turqstat_2.2.4.tar. gz Debian: http://security.debian.org/pool/updates/main/t/turqstat/ Currently we are not aware of any exploits for this vulnerability.	Turquoise SuperStat Date Parser Remote Buffer Overflow CAN-2005-2658	High	Debian Security Advisory DSA 812-1, September 15, 2005

University of California (BSD License) PostgreSQL 7.x, 8.x; Peachtree Linux release 1	Multiple vulnerabilities exist that could permit malicious users to gain escalated privileges or execute arbitrary code. These vulnerabilities are due to an error in the 'LOAD' option, a missing permissions check, an error in 'contrib/intagg,' and a boundary error in the plpgsql cursor declaration. Update to version 8.0.1, 7.4.7, 7.3.9, or 7.2.7: http://wwwmaster.postgresql.org/download/mirrors-ftp Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-71-1 Debian: http://www.debian.org/security/2005/dsa-668 Gentoo: http://security.gentoo.org/glsa/glsa-200502-08.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/postgresql/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-141.html Gentoo: http://security.gentoo.org/glsa/glsa-200502-19.xml Debian: http://security.debian.org/pool/updates/main/p/postgresql/ Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2005:040 SUSE: ftp://ftp.SUSE.com/pub/SUSE Peachtree: http://peachtree.burdell.org/updates/ Trustix: http://www.trustix.org/errata/2005/0015/ **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for these vulnerabilities.	University of California PostgreSQL Multiple Vulnerabilities CAN-2005-0227 CAN-2005-0246 CAN-2005-0244 CAN-2005-0245 CAN-2005-0247	High	PostgreSQL Security Release, February 1, 2005 Ubuntu Security Notice USN-71-1 February 01, 2005 Debian Security Advisory DSA-668-1, February 4, 2005 Gentoo GLSA 200502-08, February 7, 2005 Fedora Update Notifications, FEDORA-2005-124 & 125, February 7, 2005 Ubuntu Security Notice,e USN-79-1 , February 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005 Gentoo Linux Security Advisory, GLSA 200502-19, February 14, 2005 RedHat Security Advisory, RHSA-2005:141-06, February 14, 2005 Debian Security Advisory, DSA 683-1, February 15, 2005 Mandrakesoft, MDKSA-2005:040, February 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:005, February 18, 2005 Fedora Update Notifications, FEDORA-2005-157 &158, February 22, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005 SUSE Security Announcement, SUSE-SA:2005:027, April 20, 2005 Peachtree Linux Security Notice, PLSN-0004, April 21, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0015, April 25, 2005 **Conectiva Linux Announcement, CLSA-2005:1008, September 13, 2005**
Webmin Webmin 1.220, 1.210, 1.200; Usermin 1.150, 1.140, 1.130	A vulnerability has been reported in 'miniserv.pl' due to an input validation error in the authentication process, which could let a remote malicious user bypass certain security restrictions. Webmin: http://prdownloads.sourceforge.net/webadmin/webmin-1.230.tar.gz	Webmin / Usermin Remote PAM Authentication Bypass CAN-2005-3042	Medium	SNS Advisory No.83, September 20, 2005

	Usermin: http://prdownloads.sourceforge.net/webadmin/usermin-1.160.tar.gz Currently we are not aware of any exploits for this vulnerability.		

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
AEwebworks Dating Software aeDating 4.0, 3.2	An SQL injection vulnerability has been reported in 'search_result.php' due to insufficient sanitization of the 'Country[]' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AEwebworks aeDating SQL Injection CAN-2005-2985	Medium	Secunia Advisory: SA16831, September 16, 2005
AlstraSoft EPay Pro 2.0	A Directory Traversal vulnerability has been reported in 'index.php' due to insufficient validation of the 'read' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	EPay Pro Directory Traversal CAN-2005-3026	Medium	Security Focus, Bugtraq ID: 14871, September 19, 2005
Andrea Bugada PHP Advanced Transfer Manager 1.30	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in 'txt.php,' 'htm.php,' 'html.php,' and 'zip.php' due to insufficient sanitization of input passed to the 'current_dir' and 'filename' parameters, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in the 'test.php' script when accessed directly, which could let a remote malicious user obtain sensitive information; a vulnerability was reported because a default administrator password exists, which could let a remote malicious user upload and execute arbitrary PHP files; and a Cross-Site Scripting vulnerability was reported in 'txt.php' due to insufficient sanitization of the 'font,' 'normalfontcolor,' and 'mess[31]' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	PHP Advanced Transfer Manager Multiple Vulnerabilities CAN-2005-2997 CAN-2005-2998 CAN-2005-2999 CAN-2005-3000	High	Security Tracker Alert ID: 1014930, September 19, 2005
Apache	A vulnerability has been reported in Apache which can be exploited by remote malicious users to smuggle http requests. Conectiva: http://distro.conectiva.com.br/ atualizacoes/index.php?id=a&anuncio=000982 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: ftp://patches.sgi.com/support/free/security/advisories/	Apache HTTP Request Smuggling Vulnerability CAN-2005-1268 CAN-2005-2088	Medium	Secunia, Advisory: SA14530, July 26, 2005 Conectiva, CLSA-2005:982, July 25, 2005 Fedora Update Notification FEDORA-2005-638 & 639, August 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:129, August 3, 2005 Ubuntu Security Notice, USN-160-1, August 04, 2005 Turbolinux Security Advisory, TLSA-2005-81, August 9, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 SUSE Security Announcement,

	SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/a/apache/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **IBM has released fixes for Hardware Management Console addressing this issue. Users should contact IBM for further information.** Currently we are not aware of any exploits for this vulnerability.			SUSE-SA:2005:046, August 16, 2005 Debian Security Advisory DSA 803-1, September 8, 2005 Ubuntu Security Notice, USN-160-2, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 **Security Focus, Bugtraq ID: 14106, September 21, 2005**
Check Point Software SecurePlatform NGX R60 Build 244	A vulnerability has been reported due to improper implementation of expected firewall rules, which could let a remote malicious user bypass firewall rules. No workaround or patch available at time of publishing. There is no exploit code required.	Check Point SecurePlatform NGX Firewall Rules Bypass CAN-2005-2889	Medium	Security Focus, Bugtraq ID: 14781, September r8, 2005 **US-CERT VU#508209**
Content2Web Content2Web 1.0.1	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient validation of the 'show' parameter, which could let a remote malicious user execute arbitrary PHP code; a vulnerability was reported which could let a remote malicious user execute SQL commands; a vulnerability was reported because a remote malicious user create a specially crafted URL that will cause arbitrary scripting code to be executed by the target user's browser; and a vulnerability was reported because a remote malicious user can obtain the installation path. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Content2Web Multiple Input Validation Vulnerabilities CAN-2005-3017	Medium	Security Tracker Alert ID: 1014900, September 14, 2005
CutePHP Team CuteNews 1.4 .0	A Cross-Site Scripting vulnerability has been reported in 'data/flood.db.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	CuteNews Cross-Site Scripting CAN-2005-3009	Medium	Security Tracker Alert ID: 1014929, September 19, 2005
CutePHP Team CuteNews 1.4 .0 & prior	A vulnerability has been reported in 'inc/shows.inc.php' flood protection feature, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	CuteNews Arbitrary PHP CAN-2005-3010	High	Security Focus, Bugtraq ID: 14869, September 17, 2005
Data Center Resources Avocent CCM4850 2.1 (Firmware)	A vulnerability has been reported in the 'connect' command due to an error when restricting access to certain serial ports, which could let a remote malicious user obtain unauthorized access. Update available at: ftp://ftp.avocent.com/public/product-upgrades/ There is no exploit code required.	Data Center Resources Avocent CCM Unauthorized Access CAN-2005-2984	Medium	Secunia Advisory: SA16836, September 16, 2005
DeluxeBB DeluxeBB 1.0 5, 1.0	Several SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in SQL queries, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	DeluxeBB Multiple SQL Injection CAN-2005-2989	Medium	Security Focus, Bugtraq ID: 14851, September 15, 2005

Digital Scribe Digital Scribe 1.4	An SQL injection vulnerability has been reported in 'login.php' due to insufficient sanitization of the 'username' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Digital Scribe SQL Injection CAN-2005-2987	Medium	Security Focus, Bugtraq ID: 14843, September 15, 2005
Ensim Corporation Webppliance 3.1.1, 3.1, 3.0	An HTML injection vulnerability has been reported in 'OCW_login_username' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Ensim Webppliance 'OCW_login_ username' HTML Injection CAN-2005-3014	Medium	Security Focus, Bugtraq ID: 14836, September 14, 2005
Francisco Burzi PHP-Nuke 7.6-7.8, 7.0-7.3, 6.9, 6.5-6.7, 6.0, 5.0-5.6, 4.4.1 a, 4.3, 4.0 , 3.0, 2.5, 1.0, 0.726 -3, 0.75 -RC3	Several potential vulnerabilities have been reported in the wysiwyg editor. The impact was not specified. Updates available at: http://www.phpnuke.org/modules.php?name=Release There is no exploit code required.	PHP-Nuke WYSIWYG Editor CAN-2005-3016	Not Specified	Secunia Advisory: SA16843, September 16, 2005
Helpdesk Software Hesk 0.93, 0.92	A vulnerability has been reported in the 'PHPSESSID' parameter when accessing 'admin.php' and 'admin_main.php' because it is possible to bypass the authentication process, which could let a remote malicious user obtain sensitive information Upgrades available at: http://www.phpjunkyard.com/download.php?script=hesk There is no exploit code required; however, a Proof of Concept exploit has been published.	Hesk Authentication Bypass CAN-2005-3005	Medium	Security Focus, Bugtraq ID: 14879, September 20, 2005
Hewlett Packard Company OpenView Network Node Manager 7.50 Solaris, 7.50, 6.41 Solaris, 6.41	A vulnerability has been reported in the 'node' URI parameter of the 'OvCgi/connected Nodes.ovpl' script, which could let a remote malicious user execute arbitrary code. Revision 3: Added PHSS_33783. Added preliminary files for OV NNM 7.01, 6.4, 6.2 **Revision 4:** **Corrected files are available via ftp:** **README_HPSBMA01224_ rev1.txt** **NNM6.2_HP-UX_CGI_Script_Point_ Release_rev1.tar** **NNM6.2_HP-UX_CGI_Script_Point_ Release_rev1.tar** Workaround available at: http://support.openview.hp.com/news_archives.jsp There is no exploit code required; however, a Proof of Concept exploit script has been published.	HP OpenView Network Node Manager Remote Arbitrary Code Execution CAN-2005-2773	High	Portcullis Security Advisory, 05-014, August 25, 2005 HP Security Advisory, HPSBMA01224, August 26, 2005 HP Security Advisory, HPSBMA01224 REVISION: 3, September 13, 2005 **HP Security Advisory, HPSBMA01224 REVISION: 4, September 19, 2005**
IBM Lotus Domino Enterprise Server 6.5.2, Lotus Domino 6.5.2	Two Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of the 'BaseTarget' and 'Src' parameters before returned to the user, which could let a remote malicious user execute arbitrary HTML and script code. Updates available at: http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg1LO07850&loc=en_U S&cs=utf-8&cc=us⟨=all http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg1LO07849&loc=en_U S&cs=utf-8&cc=us⟨=all Proofs of Concept exploits have been published.	IBM Lotus Domino Cross-Site Scripting CAN-2005-3015	Medium	IBM Security Advisories, September 15, 2005

InterAKT Online MX Shop 3.2 .0	An SQL injection vulnerability has been reported in the 'pages' module due to insufficient validation of input submitted to the 'idp', 'id_ctg', and 'id_prd' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	MX Shop SQL Injection CAN-2005-3004	Medium	SYSTEM SECURE.ORG Advisory, September 17, 2005
Jean-Baptiste Lamy Py2Play 0.1.7	A vulnerability has been reported due to insufficient validation/ restriction of serialized Python objects (pickles) used when receiving objects over a peer-to-peer game network, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/ glsa/glsa-200509-09.xml There is no exploit code required.	Py2Play Object Remote Python Code Execution CAN-2005-2875	High	Gentoo Linux Security Advisory GLSA 200509-09, September
Jelsoft Enterprises vBulletin 3.0.6 and prior	An input validation vulnerability was reported that could let remote malicious users inject and execute arbitrary PHP code. Nested input passed to the 'template' parameter in 'misc.php' is not properly verified. Update to version 3.0.7: http://www.vbulletin.com/ download.php **An exploit script has been published.**	Jelsoft Enterprises vBulletin PHP Code Injection Vulnerability CAN-2005-0511	High	Secunia SA14326, February 22, 2005 **Security Focus, Bugtraq ID: 12622, September 17, 2005**
Jelsoft Enterprises VBulletin 3.0-3.0.8, 2.3.0-2.3.4, 2.2.0-2.2.9, 2.0.3, 2.0, rc 2 & rc 3, 1.0.1 lite	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of some input passed in the administration section, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported due to insufficient sanitization of some input passed in the administration section before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'avatars/icons/smileys upload functionality because it is possible to upload arbitrary files inside the web root and execute arbitrary PHP scripts. Upgrades available at: http://members.vbulletin.com/ There is no exploit code required; however, Proof of Concept exploits have been published.	vBulletin Multiple Vulnerabilities CAN-2005-3020 CAN-2005-3021 CAN-2005-3022 CAN-2005-3023 CAN-2005-3024 CAN-2005-3025	High	BuHa Security-Advisory #2 & 3, September 17, 2005
Jiba Tofu 0.2	A vulnerability has been reported due to insufficient validation/ restriction of serialized Python objects (pickles) used when receiving objects over a peer-to-peer game network, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Tofu Game Engine Arbitrary Python Code Execution CAN-2005-3008	High	Security Focus, Bugtraq ID: 14865, September 17, 20005
Mozilla Firefox 1.0.6; Mozilla Browser 1.7.11, 1.7-1.7.9	A vulnerability has been reported which could let a remote malicious user execute arbitrary commands via shell metacharacters in a URL. Upgrades available at: http://www.mozilla.org/ products/firefox/ There is no exploit code required; however, a Proof of Concept exploit has been published.	Mozilla Browser/Firefox Arbitrary Command Execution CAN-2005-2968	High	Security Focus Bugtraq ID: 14888, September 21, 2005
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'InstallTrigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM	Firefox Multiple Vulnerabilities CAN-2005-2260 CAN-2005-2261 CAN-2005-2262 CAN-2005-2263 CAN-2005-2264 CAN-2005-2265 CAN-2005-2267 CAN-2005-2269 CAN-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security

	node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-586.html Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/ http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ http://security.debian.org/pool/updates/main/m/mozilla/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-24.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ Debian: http://security.debian.org/pool/updates/main/m/mozilla/ **Fedora:**		Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005 Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 Debian Security Advisory, DSA 779-1, August 20, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005 Slackware Security Advisory, SSA:2005-085-01, August 28, 2005 Debian Security Advisory, DSA 779-2, September 1, 2005 Debian Security Advisory, DSA 810-1, September 13, 2005 **Fedora Legacy Update Advisory, FLSA:160202, September 14, 2005** **HP Security Bulletin, HPSBOV01229, September 19, 2005**

	http://download.fedoralegacy.org/fedora/ **HP:** **http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBOV01229** Exploits have been published.			
Mozilla.org Netscape 8.0.3.3, 7.2; Mozilla Firefox 1.5 Beta1, 1.0.6, Mozilla Browser 1.7.11	A buffer overflow vulnerability has been reported due to an error when handling IDN URLs that contain the 0xAD character in the domain name, which could let a remote malicious user execute arbitrary code. Patches available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-769.html http://rhn.redhat.com/errata/RHSA-2005-768.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-11.xml** A Proof of Concept exploit script has been published.	Mozilla/Netscape/Firefox Browsers Domain Name Buffer Overflow CAN-2005-2871	High	Security Focus, Bugtraq ID: 14784, September 10, 2005 RedHat Security Advisories, 769-8 & RHSA-2005:768-6, September 9, 2005 Fedora Update Notifications, FEDORA-2005-871-184, September 10, 2005 Ubuntu Security Notice, USN-181-1, September 12, 2005 US-CERT VU#573857 **Gentoo Linux Security Advisory GLSA 200509-11, September 18, 2005**
NooTopList NooTopList 1.0 .0.17	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'o' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	NooToplist SQL Injection CAN-2005-3003	Medium	Security Tracker Alert ID: 1014931, September 19, 2005
Opera Software Opera Web Browser 8.0-8.02	An unspecified drag and drop and file upload vulnerability has been reported, which could possibly lead to the execution of arbitrary code in the context of the user running the browser. Upgrades available at: http://www.opera.com/download/ Currently we are not aware of any exploits for this vulnerability.	Opera Web Browser Unspecified Drag & Drop File Upload CAN-2005-3041	Medium	Security Focus, Bugtraq ID: 14884, September 20, 2005
Opera Software Opera Web Browser 8.0 2	Several vulnerabilities have been reported: a vulnerability was reported because attached files are opened without warnings, which could let a remote malicious user execute arbitrary JavaScript code; and a vulnerability was reported because filenames can be appended with an additional '.' which could let a remote malicious user spoof attachment names. Upgrade available at: http://www.opera.com/download/ There is no exploit code required.	Opera Mail Client Attachment Spoofing & Arbitrary JavaScript Execution CAN-2005-3006 CAN-2005-3007	Medium	Secunia Advisory: SA16645, September 20, 2005
PHPNuke PHPNuke 7.8	Multiple SQL injection vulnerabilities have been reported in the 'modules.php' due to insufficient sanitization of the 'name,' 'sid,' and 'pid' parameters, which could let a remote malicious user execute arbitrary SQL code. **Upgrade available at:** **http://phpnuke.org/modules.php?name=Downloads&d_op=getit&lid=527** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPNuke Multiple SQL Injection	Medium	NewAngels Advisory #7, September 12, 2005 **Security Focus, Bugtraq ID: 14815, September 14, 2005**

Php Outsourcing Noah's Classifieds 1.3, 1.2	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'rollid'' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'rollid' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Noah's Classifieds SQL Injection & Cross-Site Scripting CAN-2005-2979 CAN-2005-2980	Medium	Secunia Advisory: SA16826, September 15, 2005
ScriptsCenter Autolinks 2.1	A vulnerability has been reported in 'al_initialize.php' due to insufficient verification of the 'alpath' parameter before used to include files, which could let a remote malicious user execute arbitrary code. **The vendor has released Autolinks 2.1.1 to address this issue. A patch is available for prior releases as well. Please contact the vendor to obtain the upgrade or patch.** There is no exploit code required; however, a Proof of Concept exploit has been published.	AutoLinks Pro Include File Remote Arbitrary Code Execution CAN-2005-2782	High	NewAngels Advisory #1, August 28, 2005 **Security Focus, Bugtraq ID: 14686, September 17, 2005**
SquirrelMail SquirrelMail 1.4.0-1.4.5-RC1.	A vulnerability has been reported in 'options_identities.php' because parameters are insecurely extracted, which could let a remote malicious user execute arbitrary HTML and script code, or obtain/manipulate sensitive information. Upgrades available at: http://www.squirrelmail.org/download.php Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-595.html Apple: http://docs.info.apple.com/article.html?artnum=302163 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Fedora:** **http://download.fedoralegacy.org/fedora/** There is no exploit code required.	SquirrelMail Variable Handling CAN-2005-2095	Medium	GulfTech Security Research Advisory, July 13, 2005 Debian Security Advisory, DSA 756-1, July 13, 2005 RedHat Security Advisory, RHSA-2005:595-12, August 3, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 Fedora Update Notifications, FEDORA-2005-779 & 780 , August 22, 2005 **Fedora Legacy Update Advisory, FLSA:163047, September 15, 2005**
SquirrelMail SquirrelMail 1.4.0 through 1.4.4	Multiple vulnerabilities have been reported that could let remote malicious users conduct Cross-Site Scripting attacks. Upgrade to 1.4.4 and apply patch: http://prdownloads.sourceforge.net/squirrelmail/sqm-144-xss.patch Gentoo: http://security.gentoo.org/glsa/glsa-200506-19.xml Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-595.html	SquirrelMail Cross-Site Scripting Vulnerabilities CAN-2005-1769	Medium	SquirrelMail Advisory, June 15, 2005 Gentoo Linux Security Advisory, GLSA 200506-19, June 21, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:108, July 1, 2005 Debian Security Advisory , DSA 756-1, July 13, 2005 RedHat Security Advisory, RHSA-2005:595-12, August 3, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005

	Apple: http://docs.info.apple.com/article.html?artnum=302163 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Fedora:** **http://download.fedoralegacy.org/fedora/** There is no exploit code required.			Fedora Update Notifications, FEDORA-2005-779 & 780 , August 22, 2005 **Fedora Legacy Update Advisory, FLSA:163047, September 15, 2005**
TWiki TWiki 20040902, 20040901, 20030201, 01-Dec-2001	A vulnerability has been reported in '/cgi-bin/view/Main/TWikiUsers' due to insufficient sanitization of the 'rev' parameter before using in a shell expression, which could let a remote malicious user execute arbitrary code. Patch available at: http://twiki.org/p/pub/Codev/SecurityAlertExecuteCommandsWithRev/TWiki200409-02-03.patch There is no exploit code required; however, a Proof of Concept exploit script has been published.	TWiki Remote Arbitrary Command Execution CAN-2005-2877	High	Security Focus, Bugtraq ID: 14834, September 14, 2005 US-CERT VU#757181
WordPress WordPress 1.5.3 & prior	A vulnerability has been reported in the 'cache_lastpostdata' parameter due to insufficient sanitization, which could let a remote malicious user execute arbitrary PHP script code. No workaround or patch available at time of publishing. **An exploit script has been published.**	WordPress PHP Code Execution CAN-2005-2612	High	Secunia Advisory: SA16386, August 10, 2005 **Security Focus, Bugtraq ID: 14533, September 17, 2005**
Zebedee Zebedee 2.4.1	A remote Denial of Service vulnerability has been reported due to a failure to handle exceptional network requests. Upgrades available at: http://prdownloads.sourceforge.net/zebedee/zebedee-2.4.1A.tar.gz?downl oad **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-14.xml** There is no exploit code required; however, an exploit script has been published.	Zebedee Remote Denial of Service CAN-2005-2904	Low	Secunia Advisory: SA16788, September 12, 2005 **Gentoo Linux Security Advisory, GLSA 200509-14, September 20, 2005**

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Hotspot Usage To Keep Growing: Study:** According to a study released by the market research firm, In-Stat, the usage and number of wireless hotspots will continue to grow at a rapid rate. The study predicted that the number of hotspots will nearly double, with almost 200,000 being available by the end of 2009. Source: http://www.mobilepipeline.com/showArticle.jhtml?articleID=171000071.

Wireless Vulnerabilities

- Cambridge Computer Corporation vxTftpSrv, a trivial ftp server for Windows CE devices, can reportedly be crashed or allow arbitrary code execution with an overly long filename.
- Cambridge Computer Corporation vxFtpSrv, an ftp server for Windows CE devices, can reportedly be crashed or allow arbitrary code execution with a special USER command triggering a buffer overflow.
- Cambridge Computer Corporation vxWeb, a web server for Windows CE devices, can reportedly be crashed with a special HTTP GET command triggering a buffer overflow.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse	Script name	Workaround or Patch Available	Script Description

Chronological Order)			
September 20, 2005	myspace-dyn0.txt	No	Exploitation details for the Myspace.com Cross-Site Scripting vulnerability.
September 20, 2005	twikivuln.txt	Yes	Detailed exploitation for the TWiki Remote Arbitrary Command Execution vulnerability.
September 20, 2005	yersinia-0.5.5.1.tgz	N/A	Yersinia implements several attacks for the following protocols: Spanning Tree (STP), Cisco Discovery (CDP), Dynamic Host Configuration (DHCP), Hot Standby Router (HSRP), Dynamic Trunking (DTP), 802.1q and VLAN Trunking (VTP), helping a pen-tester with different tasks.
September 19, 2005	cutenxpl.php	No	Proof of Concept exploit for the CuteNews PHP Code Injection vulnerability.
September 17, 2005	php_vbulletin_template.pm	Yes	Exploit for the Jelsoft Enterprises vBulletin PHP Code Injection Vulnerability.
September 17, 2005	php_wordpress_lastpost.pm	No	Exploit for the WordPress PHP Code Execution vulnerability.

[back to top]

Trends

- **Keystrokes Reveal Passwords to Researchers:** According to researchers at the University of California, Berkeley, a way to eavesdrop on your computer has been figured out simply by listening to the clicks and clacks of the keyboard. When processed by a computer, those seemingly random noises were translated with up to 96 percent accuracy. Source: http://abcnews.go.com/Technology/wireStory?id=1143289.
- **Banks face customer exodus if hacked:** According to a new survey by EDS, more than half of US banking customers would stop using their bank if it suffered a successful hacking attack. Source: http://www.vnunet.com/vnunet/news/2142582/banks-face-consumer-exodus .
- **Serial typo-squatters target security firms:** The computer security industry appears to have been targeted by a serial typo-squatter by registering domain names which are similar in all but one or two characters to the domains of companies such as Computer Associates, F-Secure, McAfee, MessageLabs and Symantec. Symantec's Norton AntiVirus products appear to be the main target, with more than 100 variations registered, such as Nortonaantivirus.com. Source: http://news.zdnet.com/2100-1009_22-5873001.html.
- **Mass-mailed email greeting card leads to malware infection, Sophos reports:** SophosLabs experts are warning users of an electronic greeting card that has been spammed out to email addresses around the world, but really attempts to install a Trojan horse onto recipients' computers. Source: http://www.sophos.com/virusinfo/articles/ecard.html.
- **Bagle variant floods inboxes worldwide:** Businesses are being urged to update their antivirus protection after the author of a new Bagle variant, BagleDL-U Trojan, launched two mass spamming campaigns to spread the malware. The Trojan is enclosed in an email that contains no header and the message reads 'new price' and contains a zipped attachment. Source: http://www.vnunet.com/vnunet/news/2142560/bagle-author-tries-again.
- **Tremendous growth of cybercrime, report says:** According to a survey conducted by Symantec. Corp. online criminal activity of nearly every variety surged in the first half of 2005. This was due to an increase in software security flaws and in the number of home computers being used against their owners' wishes to distribute spam, spyware and viruses. Source: http://www.crime-research.org/news/20.09.2005/1500/.
- **Worm spoofs Google on infected PCs:** A worm, P2Load-A, has been developed by virus writers that spoofs the behavior of internet search engine Google. The HOSTS file on infected PCs is replaced with a file downloaded from a remote website that is under the control of hackers. Source: http://www.securityfocus.com/news/11322.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
3	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.

4	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
5	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
6	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
7	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
8	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
9	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
10	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.

Table Updated September 21, 2005

[back to top]

Last updated September 22, 2005