Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so 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.

  - **Multiple Vendors Linux Kernel Stack Fault Exceptions Denial of Services (Updated)**
  - **Multiple Vendors Linux Kernel 'ptrace()' Denial of Service (Updated)**
  - **Zlib Compression Library Buffer Overflow (Updated)**
  - **Multiple Vendors GDB Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel Race Condition and Buffer Overflow (Updated)**
  - **Multiple Vendors Linux Kernel Netfilter Memory Leak Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel 64 Bit 'AR-RSC' Register Access (Updated)**
  - **Multiple Vendors Linux Kernel Moxa Char Driver Buffer Overflows (Updated)**
  - **Multiple Vendors Linux Kernel Local DRM Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel EXT2 File System Information Leak (Updated)**
  - **Multiple Vendors Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel IPSec Policies Authorization Bypass (Updated)**
  - Multiple Vendors Linux Kernel routing_ioctl() Denial of Service
  - Multiple Vendors Linux Kernel USB Subsystem Denials of Service
  - **Multiple Vendors XFree86 Pixmap Allocation Buffer Overflow (Updated)**
  - **Net-SNMP Fixprox Insecure Temporary File Creation (Updated)**
  - **PCRE Regular Expression Heap Overflow (Updated)**
  - Qpopper Privilege Elevation
  - RSyslog SQL Injection
  - Script Solutions PerlDiver Perldiver.CGI Cross-Site Scripting
  - **slocate Long Path Denial of Service (Updated)**
  - Sun Solaris Xsun & Xprt Elevated Privileges
  - Sun Solaris UFS Local Denial of Service
  - **Webmin / Usermin Remote PAM Authentication Bypass (Updated)**
  - **Winace UnAce ACE Archive Remote Directory Traversal & Buffer Overflow (Updated)**
  - Yukihiro Matsumoto Ruby Safe Level Restrictions Bypass
- Multiple Operating Systems
  - AlstraSoft E-Friends Remote File Include
  - **Barracuda Spam Firewall Remote Directory Traversal & Remote Command Execution (Updated)**
  - **Cisco IOS Firewall Authentication Proxy Buffer Overflow (Updated)**
  - CJ LinkOut Cross-Site Scripting
  - CJ Tag Board Multiple Cross-Site Scripting
  - CJ Web2Mail Multiple Cross-Site Scripting
  - **CMS Made Simple Authentication Bypass & File Include (Updated)**
  - CMS Made Simple Cross-Site Scripting
  - ContentServ Local File Include
  - GeSHI Directory Traversal
  - IBM Lotus Domino Cross-Site Scripting
  - JPortal SQL Injection
  - Land Down Under Multiple Remote SQL Injection
  - LucidCMS Cross-Site Scripting
  - Microsoft Internet Explorer for Mac OS Remote Denial of Service
  - **Mozilla Browser/Firefox Arbitrary Command Execution (Updated)**

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
7-Zip 3.13, 4.23, and Beta 4.26	A buffer overflow vulnerability has been reported in 7-Zip, ARJ archive processing, that could let remote malicious users execute arbitrary code. Upgrade to the newest version: http://www.7-zip.org/ Currently we are not aware of any exploits for this vulnerability.	7-Zip Arbitrary Code Execution CAN-2005-3051	High	Secunia, Advisory: SA16664, September 23, 2005
ConeXware PowerArchiver 2006 9.5 Beta 4, Beta 5, PowerArchiver 2004 9.25, PowerArchiver 2003 8.60, PowerArchiver 2002 8.10	A buffer overflow vulnerability has been reported in PowerArchiver, ARJ and ACE archive processing, that could let remote malicious users execute arbitrary code. Upgrade to the newest version: http://www.powerarchiver.com/download/ Currently we are not aware of any exploits for this vulnerability.	PowerArchiver Arbitrary Code Execution CAN-2005-3061	High	Secunia Advisory: SA16713
FL Studio 5.0.1, 5.0.2	A buffer overflow has been reported in FL Studio, FLP file handling, that could let remote malicious users to execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	FL Studio Arbitrary Code Execution CAN-2005-3092	High	Secunia, Advisory: SA16958, September 27, 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. **Upgrade to version 1.2 http://www.handyaddressbook.com/downloads/AHABS12.exe** 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 **Security Focus, ID: 14818, September 26, 2005**
Novell GroupWise 6.5.3	A vulnerability has been reported in GroupWise that could let local malicious users execute arbitrary code. Upgrade to version 6.5 SP5: http://support.novell.com/filefinder/16963/beta.html Currently we are not aware of any exploits for this vulnerability.	Novell GroupWise Arbitrary Code Execution CAN-2005-2804	High	Security Tracker, Alert ID: 1014977, September 27, 2005

SecureW2 3.0, 3.1.1	A vulnerability has been reported in SecureW2 that could let remote malicious users to disclose sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	SecureW2 Information Disclosure CAN-2005-3087	Medium	Secunia, Advisory: SA16909, September 26, 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 **USCERT VU# 927793, 620497, September 22, 2005**

[back to top]

UNIX / Linux Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Alkalay.net nslookup.cgi, notify, man-cgi, contribute.pl	Multiple vulnerabilities have been reported: a vulnerability was reported in various perl scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; and a Directory Traversal vulnerability was reported in 'contribute.cgi' (aka contribute.pl), dated 16 Jun 2002, which could 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.	Alkalay.Net Multiple Scripts Arbitrary Remote Command Execution & Directory Traversal CAN-2005-3094 CAN-2005-3095 CAN-2005-3096 CAN-2005-3097	High	CIRT-200504 Advisory, September 21, 2005
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	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

	&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/ 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 **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf** There is no exploit code required.			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, 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 **Avaya Security Advisory, ASA-2005-204, September 23, 2005**
Apple Mac OS X Server 10.4-10.4.2, 10.3-10.3.9, Mac OS X 10.4-10.4.2, 10.3-10.3.9	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'ImageIO' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in 'Mail.app' when processing auto-reply rules, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in 'Mail.app' when using Kerberos 5 for SMTP authentication, which could let a remote malicious user obtain	Apple Mac OS X Security Update CAN-2005-1992 CAN-2005-2524 CAN-2005-2741 CAN-2005-2742 CAN-2005-2743 CAN-2005-2744 CAN-2005-2745 CAN-2005-2746 CAN-2005-2747 CAN-2005-2748	High	Apple Security Advisory, LE-SA-2005-09-22, September 22, 2005 US-CERT VU#650681 US-CERT VU#529945

	sensitive information; a vulnerability was reported because 'malloc' creates diagnostic files insecurely when using certain environmental variables to enable debugging of application memory allocation, which could let a malicious user overwrite arbitrary files; a buffer overflow vulnerability was reported in the 'QuickDraw' manager due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the Java extensions that are bundled with Quick Time 6.52 & prior due to a validation error, which could let untrusted applets call arbitrary functions from system libraries; a vulnerability was reported in Ruby, which could let a remote malicious user bypass certain security restrictions; a Cross-Site Scripting vulnerability was reported in Safari when web archives are rendered from a malicious site, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in the 'SecurityAgent' due to an error, which could let a malicious user obtain unauthorized access to a current user's desktop; and a vulnerability was reported in the Authorization Services 'securityd' due to a validation error, which could let a malicious user obtain elevated privileges. Update information available at: http://docs.info.apple.com/article.html?artnum=302413 Currently we are not aware of any exploits for these vulnerabilities.			
Astaro Corporation Astaro Security Linux 4.0 27	A remote Denial of Service vulnerability has been reported in the Point-to-Point Tunneling Protocol (PPTP) server due to an unspecified error. Upgrade available at: ftp://ftp.astaro.com/pub/Astaro_Security_Linux/v4.0/up2date/4.028.tar.gpg Currently we are not aware of any exploits for this vulnerability.	Astaro Security Linux PPTP Server Unspecified Remote Denial of Service CAN-2005-3100	Low	Security Focus, Bugtraq ID: 14950, September 27, 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	ClamAV UPX Buffer Overflow & FSG Handling Denial of Service	High	Secunia Advisory: SA16848, September 19, 2005 Gentoo Linux Security Advisory, GLSA

	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 **Mandriva:** **http://www.mandriva.com/security/advisories** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for these vulnerabilities.	CAN-2005-2919 CAN-2005-2920		200509-13, September 19, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:166, September 20, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0051, September 23, 2005**
Detlev Offenbach eric3 prior to 3.7.2	A vulnerability has been reported due to a "potential security exploit." The impact was not specified Upgrades available at: http://prdownloads.sourceforge.net/eric-ide/eric-3.7.2.tar.gz?download Currently we are not aware of any exploits for this vulnerability.	eric3 Unspecified Vulnerability CAN-2005-3068	Not Specified	Security Tracker Alert ID: 1014947, September 21, 2005
Easy Software Products CUPS 1.1.21, 1.1.22 rc1, 1.1.22	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted HTTP GET request. Upgrades available at: http://www.cups.org/software.php?SOFTWARE=v1_2 **Fedora:** **http://download.fedora.redhat.com/pub/fedora/inux/core/updates/3/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-772.html** A Proof of Concept exploit has been published.	CUPS HTTP GET Denial of Service CAN-2005-2874	Low	Security Tracker Alert ID, 1012811, January 7, 2005 **Fedora Update Notification, FEDORA-2005-908, September 22, 2005** **RedHat Security Advisory, RHSA-2005:772-8, September 27, 2005**
GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a	GNU GZip Directory Traversal	Medium	Bugtraq, 396397, April 20, 2005 Ubuntu Security Notice,

	file with the '-N' flag, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.009-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/g/gzip Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1 Avaya: http://support.avaya.	CAN-2005-1228		USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Security Focus,13290, May 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.009, June 10, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005 Debian Security Advisory DSA 752-1, July 11, 2005 Sun(sm) Alert Notification Sun Alert ID: 101816, July 20, 2005 Avaya Security Advisory, ASA-2005-172, August 29, 2005 **Sun(sm) Alert Notification** **Sun Alert ID: 101816, Updated September 27, 2005**

	com/elmodocs2/security/ASA-2005-172.pdf **Sun: Updated Relief/Workaround section.** A Proof of Concept exploit has been published.			
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 **An 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 **Security Focus, Bugtraq ID: 14794, September 26, 2005**
GNU gzip 1.2.4, 1.3.3	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva:	GNU GZip File Permission Modification CAN-2005-0988	Medium	Security Focus, 12996, April 5, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Conectiva Linux Announce-ment,

	ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/g/gzip/gzip Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1 Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-172.pdf **Sun: Updated Relief/Workaround section.** There is no exploit code required.			CLSA-2005:974, July 6, 2005 Debian Security Advisory DSA 752-1, July 11, 2005 Sun(sm) Alert Notification Sun Alert ID: 101816, July 20, 2005 Avaya Security Advisory, ASA-2005-172, August 29, 2005 **Sun(sm) Alert Notification** **Sun Alert ID: 101816, Updated September 27, 2005**
GNU wget 1.9.1	A vulnerability exists which could permit a remote malicious user to create or overwrite files on the target user's system. Wget does not properly validate user-supplied input. A remote user can bypass the filtering mechanism if DNS can be modified so that '..' resolves to an IP address. A specially crafted HTTP response can include control characters to overwrite portions of the terminal window. SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandriva: http://www.mandriva.com/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/w/wget/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-771.html** A Proof of Concept exploit script	GNU wget File Creation & Overwrite CAN-2004-1487 CAN-2004-1488	Medium	Security Tracker Alert ID: 1012472, December 10, 2004 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:098, June 9, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 Turbolinux Security Advisory, TLSA-2005-66, June 15, 2005 Ubuntu Security Notice, USN-145-1, June 28, 2005 Ubuntu Security Notice, USN-145-2, September 06, 2005 **RedHat Security Advisory, RHSA-2005:771-10, September 27, 2005**

	has been published.			
Hylafax Hylafax 4.2.1	Several vulnerabilities have been reported: a vulnerability was reported in the 'xferfaxstats' script due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files; and a vulnerability was reported because ownership of the UNIX domain socket is not created or verified, which could let a malicious user obtain sensitive information and cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required.	HylaFAX Insecure Temporary File Creation CAN-2005-3069 CAN-2005-3070	Medium	Security Focus, Bugtraq ID: 14907, September 22, 2005
IBM AIX 5.3 L, 5.3, 5.2.2, 5.2 L, 5.2	A buffer overflow vulnerability has been reported due to a failure to perform boundary checks prior to copying user-supplied data into insufficiently-sized memory buffers, which could let a malicious user execute arbitrary code. Update information available at: http://www-1.ibm.com/support/docview.wss?uid=isg1IY73850 http://www-1.ibm.com/support/docview.wss?uid=isg1IY73814 Currently we are not aware of any exploits for this vulnerability.	IBM AIX Buffer Overflow CAN-2005-3060	High	IBM Security Advisory, September 28, 2005
Info-ZIP UnZip 5.52	A vulnerability has been reported due to a security weakness when extracting an archive to a world or group writeable directory, which could let a malicious user modify file permissions. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **SCO:** **ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.39/507** There is no exploit code required.	Info-ZIP UnZip File Permission Modification CAN-2005-2475	Medium	Security Focus, 14450, August 2, 2005 Fedora Update Notification, FEDORA-2005-844, September 9, 2005 **SCO Security Advisory, SCOSA-2005.39, September 28, 2005**
Inter7 SqWebMail 5.0.4	A vulnerability has been reported because the '<script>' tag can be used in HTML comments, which could let a remote malicious user execute arbitrary code when malicious email is viewed. Patch available at:	SqWebMail HTML Email Script Tag Script Injection CAN-2005-2820	Medium	Secunia Advisory: SA16704, September 6, 2005 **Debian Security Advisory DSA 820-1, September 24, 2005**

	http://www.courier-mta.org/beta/sqwebmail/ **Debian:** **http://security.debian.org/pool/updates/main/c/courier/** There is no exploit code required; however, a Proof of Concept exploit has been published.			
Interchange Interchange 5.2 , 5.0.1	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'pages/forum/submit.html' due to insufficient sanitization of certain parameters, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'pages/forumm/submit.html' due to an unspecified error, which could let a remote malicious user inject ITL (Interchange Tag Language) code. Upgrades available at: http://ftp.icdevgroup.org/interchange/ There is no exploit code required.	Interchange SQL Injection & ITL Injection CAN-2005-3072 CAN-2005-3073	Medium	Secunia Advisory: SA16923, September 23, 2005
KDE KDE 3.2.0 up to including 3.4.2	A vulnerability has been reported in 'kcheckpass.c' due to the insecure creation of the lock file, which could let a malicious user obtain superuser privileges. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/post-3.4.2-kdebase-kcheckpa ss.diff Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/k/kdebase/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/k/kdebase/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code	KDE kcheckpass Superuser Privilege Escalation CAN-2005-2494	High	KDE Security Advisory, September 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:160, September 6, 2005 Ubuntu Security Notice, USN-176-1 September 07, 2005 Slackware Security Advisory, SSA:2005-251-01 & 251-03, September 9, 2005 Debian Security Advisory DSA 815-1, September 16, 2005 **Conectiva Linux Announcement, CLSA-2005:1011, September 23, 2005**

	required.			
KDE KDE 3.0 - 3.4.2	A vulnerability was reported in 'langen2kvtml' due to the insecure creation of temporary files, which could let malicious user obtain elevated privileges. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/ **Debian:** **http://security.debian.org/pool/updates/main/k/kdeedu/** There is no exploit code required.	KDE langen2kvtml Insecure Temporary File Creation CAN-2005-2101	Medium	KDE Security Advisory, August 15, 2005 Fedora Update Notification, FEDORA-2005-745, August 15, 2005 Fedora Update Notifications, FEDORA-2005-744 & 745, August 16, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:159, September 6, 2005 Slackware Security Advisory, SSA:2005-251-03, September 9, 2005 **Debian Security Advisory, DSA 818-1, September 22, 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/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** 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 **Conectiva Linux Announcement, CLSA-2005:1012, September 23, 2005**

Multiple Vendors Linux kernel 2.6.10, 2.6.9; RedHat Fedora Core2&3	A Denial of Service vulnerability exists in the 'mlockall()' system call due to a failure to properly enforce defined limits. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-663.html** A Proof of Concept exploit script has been published.	Linux Kernel Local RLIMIT_MEMLOCK Bypass Denial of Service CAN-2005-0179	Low	Bugtraq, January 7, 2005 Fedora Update Notifications, FEDORA-2005-013 & 014, January 10, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 Conectiva Linux Security Announcement, CLA-2005:930, March 7, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11	Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html Conectiva: ftp://atualizacoes.conectiva.com.br/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-663.html** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities CAN-2005-0815	High	Security Focus, 12837, March 18, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Ubuntu Security Notice, USN-103-1, April 1, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**

Multiple Vendors RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Linux kernel 2.6.9, 2.6-2.6.8	A Denial of Service vulnerability has been reported in the auditing code. RedHat: http://rhn.redhat.com/errata/RHSA-2005-420.html **RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Auditing Code Denial of Service CAN-2005-0136	Low	RedHat Security Advisory, RHSA-2005:420-22, June 8, 2005 RedHat Security Advisory, RHSA-2005:420-24, Updated August 9, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**
Multiple Vendors RedHat Fedora Core4, Core3, Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Real Networks RealPlayer For Unix 10.0.4, 10.0.3, RealPlayer 10 for Linux , Japanese, German, English, Helix Player for Linux 1.0-1.0.4	A format string vulnerability has been reported when displaying an invalid-handle error message, which could let a remote malicious user execute arbitrary code. RedHat: http://rhn.redhat.com/errata/RHSA-2005-788.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ An exploit script has been published.	RealNetworks RealPlayer & Helix Player Format String CAN-2005-2710	High	RedHat Security Advisory, RHSA-2005:788-3, September 27, 2005 Fedora Update Notifications, FEDORA-2005-940 & 941, September 27,2005 US-CERT VU#361181
Multiple Vendors SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12	A buffer overflow vulnerability has been reported in the XFRM network architecture code due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code. Patches available at: http://www.kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel XFRM Array Index Buffer Overflow CAN-2005-2456	High	Security Focus, 14477, August 5, 2005 Ubuntu Security Notice, USN-169-1, August 19, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**
Multiple Vendors SuSE Linux Professional 9.0, x86_64; Linux kernel 2.6-2.6.12,	An unspecified Denial of Service vulnerability has been reported when stack fault exceptions are triggered. SUSE: ftp://ftp.SUSE.com/	Linux Kernel Stack Fault Exceptions Denial of Service CAN-2005-1767	Low	Security Focus, 14467, August 3, 2005 SUSE Security Announcement, SUSE-SA:2005:044,

2.5 .0- 2.5.69, 2.4-2.4.32	pub/SUSE **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-663.html** Currently we are not aware of any exploits for this vulnerability.			August 4, 2005 **Ubuntu Security Notice, USN-187-1, September 25, 2005** **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**

Multiple Vendors
Ubuntu Linux 5.0 4 amd64, 4.1 ia64;
SuSE Linux 9.3 x86_64, 9.1 x86_64, 9.0 x86_64;
Linux kernel 2.6.10, 2.6.8
	A Denial of Service has been reported in 'ptrace()' due to insufficient validation of memory addresses.
	Updates available at:
	http://kernel.org/
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-663.html
	Currently we are not aware of any exploits for this vulnerability.
		Linux Kernel 'ptrace()' Denial of Service
		CAN-2005-0756
			Low	Ubuntu Security Notice, USN-137-1, June 08, 2005
				SUSE Security Announcement, SUSE-SA:2005:029, June 9, 2005
				RedHat Security Advisory, RHSA-2005:663-19, September 28, 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: 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	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 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

	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/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-18.xml** Currently we are not aware of any exploits for this vulnerability.			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 **Gentoo Linux Security Advisory, GLSA 200509-18, September 26, 2005**
Multiple Vendors Gentoo Linux; GNU GDB 6.3	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when loading malformed object files, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported which could let a malicious user obtain elevated privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200505-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gdb/ http://security.ubuntu.com/ubuntu/pool/main/b/binutils/ Mandriva: http://www.mandriva.com/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/	GDB Multiple Vulnerabilities CAN-2005-1704 CAN-2005-1705	High	Gentoo Linux Security Advisory, GLSA 200505-15, May 20, 2005 Turbolinux Security Advisory, TLSA-2005-68, June 22, 2005 **RedHat Security Advisory, RHSA-2005:659-9, September 28, 2005**

	TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-659.html** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Linux Kernel 2.4, 2.6	A race condition vulnerability has been reported in ia32 emulation, that could let local malicious users obtain root privileges or create a buffer overflow. Patch Available: http://kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32-pre1.bz2 Trustix: http://http.trustix.org/pub/trustix/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-663.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Race Condition and Buffer Overflow CAN-2005-1768	High	Security Focus, 14205, July 11, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005 SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**
Multiple Vendors Linux kernel 2.6 .10, Linux kernel 2.6 -test1-test11, 2.6-2.6.8	A Denial of Service vulnerability has been reported in the Netfilter code due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ SuSE: ftp://ftp.suse.com/pub/suse/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat:	Linux Kernel Netfilter Memory Leak Denial of Service CAN-2005-0210	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory,

	http://rhn.redhat.com/ errata/RHSA-2005-366.html **RedHat: http://rhn.redhat.com/ errata/RHSA- 2005-663.html** Currently we are not aware of any exploits for this vulnerability.			RHSA-2005 :366-21, August 9, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**
Multiple Vendors Linux kernel 2.6 prior to 2.6.12.1	A vulnerability has been reported in the 'restore_sigcontext()' function due to a failure to restrict access to the 'ar.rsc' register, which could let a malicious user cause a Denial of Service or obtain elevated privileges. Updates available at: http://www.kernel.org/ SUSE: http://www.novell.com/linux/ security/advisories/ 2005_44_kernel.html **RedHat: http://rhn.redhat.com/ errata/RHSA- 2005-663.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 64 Bit 'AR-RSC' Register Access CAN-2005-1761	Medium	Security Tracker Alert ID: 1014275, June 23, 2005 SUSE Security Announce- ment, SUSE-SA:2005:044, August 4, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**
Multiple Vendors Linux Kernel 2.2, 2.4, 2.6	Several buffer overflow vulnerabilities exist in 'drivers/char/moxa.c' due to insufficient validation of user-supplied inputs to the 'MoxaDriverIoctl(),' ' moxaloadbios(),' moxaloadcode(),' and 'moxaload320b()' functions, which could let a malicious user execute arbitrary code with root privileges. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ linux-source-2.6.8.1/l SUSE: ftp://ftp.SUSE.com/ pub/SUSE FedoraLegacy: http://download.fedoralegacy. org/redhat/ **RedHat: http://rhn.redhat.com/ errata/RHSA- 2005-663.html** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Moxa Char Driver Buffer Overflows CAN-2005-0504	High	Security Tracker Alert, 1013273, February 23, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**

Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The DRM module in the Linux kernel is susceptible to a local Denial of Service vulnerability. This vulnerability likely results in the corruption of video memory, crashing the X server. Malicious users may be able to modify the video output. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html FedoraLegacy: http://download.fedoralegacy.org/redhat/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Local DRM Denial of Service CAN-2004-1056	Low	Ubuntu Security Notice USN-38-1 December 14, 2004 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test 11, 2.6.1-2.6.11; RedHat Fedora Core2	A vulnerability has been reported in the EXT2 filesystem handling code, which could let malicious user obtain sensitive information. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html Conectiva: ftp://atualizacoes.conectiva.com.br/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ SUSE: ftp://ftp.SUSE.com/pub/SUSE	Linux Kernel EXT2 File System Information Leak CAN-2005-0400	Medium	Security Focus, 12932, March 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005 SUSE Security Announcement, SUSE-SA:2005:029, June 9, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**

	RedHat: **http://rhn.redhat.com/errata/RHSA-2005-663.html** Currently we are not aware of any exploits for this vulnerability.			
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/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-663.html** 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 **Fedora Update Notifications, FEDORA-2005-905 & 906, September 22, 2005** **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12 .1	A vulnerability has been reported due to insufficient authorization before accessing a privileged function, which could let a malicious user bypass IPSEC policies. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ This issue has been addressed in Linux kernel 2.6.13-rc7. SUSE: ftp://ftp.SUSE.com/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-663.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPSec Policies Authorization Bypass CAN-2005-2555	Medium	Ubuntu Security Notice, USN-169-1, August 19, 2005 Security Focus, Bugtraq ID 14609, August 19, 2005 Security Focus, Bugtraq ID 14609, August 25, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 **RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005**

Multiple Vendors Linux kernel 2.6-2.6.13.1	A Denial of Service vulnerability has been reported due to an omitted call to the 'sockfd_put()' function in the 32-bit compatible 'routing_ioctl()' function. Fixed version (2.6.13.2), available at: http://kernel.org/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel routing_ioctl() Denial of Service CAN-2005-3044	Low	Security Tracker Alert ID: 1014944, September 21, 2005 Ubuntu Security Notice, USN-187-1, September 25, 2005
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported when handling asynchronous USB access via usbdevio; and a Denial of Service vulnerability was reported in the 'ipt_recent.c' netfilter module due to an error in jiffies comparison. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel USB Subsystem Denials of Service CAN-2005-2873 CAN-2005-3055	Low	Secunia Advisory: SA16969, September 27, 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
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Trustix:
	http://http.trustix.org/pub/trustix/updates/
	Debian:
	http://security.debian.org/pool/updates/main/x/xfree86/
	Sun:
	http://sunsolve.sun.com/search/document.do?assetkey=1-26-101926-1&searchclause
	SUSE:
	ftp://ftp.suse.com/pub/suse/
	Slackware:
	ftp://ftp.slackware.com/pub/slackware/
	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
				Fedora Update Notifications, FEDORA-2005-893 & 894, September 16, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005
				Debian Security Advisory DSA 816-1, September 19, 2005
				Sun(sm) Alert Notification
				Sun Alert ID: 101926, September 19, 2005
				SUSE Security Announcement, SUSE-SA:2005:056, September 26, 2005
				Slackware Security Advisory, SSA:2005-269-02, September 26, 2005

Net-snmp Net-snmp 5.x	A vulnerability has been reported in 'fixproc' due to a failure to securely create temporary files in world writeable locations, which could let a malicious user obtain elevated privileges and possibly execute arbitrary code with ROOT privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200505-18.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **https://rhn.redhat.com/** There is no exploit code required.	Net-SNMP Fixprox Insecure Temporary File Creation CAN-2005-1740	High	Gentoo Linux Security Advisory, GLSA 200505-18, May 23, 2005 Fedora Update Notifications, FEDORA-2005-561 & 562, July 13, 2005 **RedHat Security Advisory, RHSA-2005:373-23, September 28, 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/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**	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 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

	.org/glsa/glsa-200509-12.xml **Debian:** **http://security.debian.org/pool/updates/main/p/python2.2/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-19.xml** **Debian:** **http://security.debian.org/pool/updates/main/p/python2.3/** Currently we are not aware of any exploits for this vulnerability.			**Debian Security Advisory, DSA 817-1 & DSA 819-1, September 22 & 23, 2005** **Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005** **Debian Security Advisory, DSA 821-1, September 28, 2005**
Qualcomm qpopper 4.0.8	A vulnerability has been reported in the 'poppassd' setuid-superuser application, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Qpopper Privilege Elevation CAN-2005-3098	Medium	Security Focus, Bugtraq ID: 14944, September 26, 2005
RSyslog RSyslog 1.10 , 0.9.3 -0.9.8	An SQL injection vulnerability has been reported due to insufficient sanitization of a received syslog message before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://www.rsyslog.com/Downloads-index-req-getit-lid-17.phtml There is no exploit code required.	RSyslog SQL Injection CAN-2005-3074	Medium	Secunia Advisory: SA16947, September 26, 2005
Script Solutions PerlDiver 2.31	A Cross-Site Scripting vulnerability has been reported in 'Perldiver.cgi' due to insufficient sanitization of the 'module' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://www.scriptsolutions.com/support/ There is no exploit code required; however, Proof of Concept exploits have been published.	PerlDiver Perldiver.CGI Cross-Site Scripting CAN-2005-3066 CAN-2005-3067	Medium	EXPL-A-2005-014 exploitlabs.com Advisory 043, September 21, 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/ **RedHat:** **https://rhn.redhat.com/** 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 **RedHat Security Advisory, RHSA-2005:345-24, September 28, 2005**
Sun Microsystems Inc. Solaris 10.0, _x86, 9.0, _x86, 8.0, _x86, 7.0, _x86	A vulnerability has been reported in the Xsun and Xprt commands due to an unspecified error, which could let a malicious user obtain elevated privileges. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101800-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris Xsun & Xprt Elevated Privileges CAN-2005-3099	Medium	Sun(sm) Alert Notification Sun Alert ID: 101800, September 26, 2005
Sun Microsystems, Inc. Solaris 9.0, _x86, 8.0, _x86	A Denial of Service vulnerability has been reported due to an unspecified error in the UFS (Unix File System). Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101940-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris UFS Local Denial of Service CAN-2005-3071	Low	Sun(sm) Alert Notification Sun Alert ID: 101940, September 22, 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 Usermin: http://prdownloads.sourceforge.net/webadmin/usermin-1.160.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-17.xml**	Webmin / Usermin Remote PAM Authentication Bypass CAN-2005-3042	Medium	SNS Advisory No.83, September 20, 2005 **Gentoo Linux Security Advisory, GLSA 200509-17, September 24, 2005**

	Currently we are not aware of any exploits for this vulnerability.			
winace.com UnAce 1.0, 1.1, 1.2 b	Several vulnerabilities exist: a buffer overflow vulnerability exists in the ACE archive due to an incorrect 'strncpy()' call, which could let a remote malicious user execute arbitrary code; two other buffer overflow vulnerabilities exist when archive name command line arguments are longer than 15,600 characters and when printing strings are processed, which could let a remote malicious user execute code; and a Directory Traversal vulnerability exists due to improper filename character processing, which could let a remote malicious user obtain sensitive information. Gentoo: http://security.gentoo.org /glsa/glsa-200502-32.xml SUSE: ftp://ftp.SUSE.com/ pub/SUSE There is not exploit code required; however, Proof of Concept exploits have been published.	Winace UnAce ACE Archive Remote Directory Traversal & Buffer Overflow CAN-2005-0160 CAN-2005-0161	High	Security Tracker Alert, 1013265, February 23, 2005 SUSE Security Summary Report, SUSE-SR:2005:016, June 17, 2005 **US-CERT VU#215006**
Yukihiro Matsumoto Ruby 1.6 - 1.6.8, 1.8 - 1.8.2	A vulnerability has been reported in 'eval.c' due to a flaw in the logic that implements the SAFE level checks, which could let a remote malicious user bypass access restrictions to execute scripting code. Patches available at: ftp://ftp.ruby-lang.org/ pub/ruby/1.6/ 1.6.8-patch1.gz Updates available at: http://www.ruby-lang.org/ patches/ruby-1.8.2- xmlrpc-ipimethods-fix.diff There is no exploit code required.	Ruby Safe Level Restrictions Bypass CAN-2005-2337	Medium	Security Tracker Alert ID: 1014948, September 21, 2005

[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
AlstraSoft E-Friends 4.0	A vulnerability has been reported in 'index.php' due to insufficient verification of the 'mode' parameter, which could let a remote malicious user include arbitrary files.	AlstraSoft E-Friends Remote File Include CAN-2005-3062	Medium	Security Focus, Bugtraq ID: 14932, September 24, 2005

	No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.			
Barracuda Networks Barracuda Spam Firewall 3.1.17 firmware	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in 'IMG.PL' which could let a remote malicious user obtain sensitive information; and a vulnerability was reported when user-supplied commands are submitted to the web interface, which could let a remote malicious user execute arbitrary commands. The vendor has released firmware version 3.1.18 to address this and other issues. Please contact the vendor to obtain the upgrade. **A Proof of Concept exploit script has been published.**	Barracuda Spam Firewall Remote Directory Traversal & Remote Command Execution CAN-2005-2847 CAN-2005-2848 CAN-2005-2849	High	Security Focus, Bugtraq ID: 14710 & 14712, September 1, 2005 **Security Focus, Bugtraq ID: 14712, September 26, 2005**
Cisco Systems Cisco IOS 12.2ZH & 12.2ZL based trains, 12.3 based trains, 12.3T based trains, 12.4 based trains, 12.4T based trains	A buffer overflow vulnerability has been reported in the authentication proxy, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml **Rev. 1.1: Added 12.2SG, 12.2SEC, and 12.2SXF releases to Software Version and Fixes table.** **Rev. 1.2: In Software Versions and Fixes table: 12.2ZH changed to 12.2SH, added 12.2ZF.** Currently we are not aware of any exploits for this vulnerability.	Cisco IOS Firewall Authentication Proxy Buffer Overflow CAN-2005-2841	High	Cisco Security Advisory, Document ID: 66269, September 7, 2005 US-CERT VU#236045 **Cisco Security Advisory, Document ID: 66269 Rev 1.1 & 1.2, September 22 & 26, 2005**
CJ Design CJ LinkOut 1.0	A Cross-SIte Scripting vulnerability has been reported in 'Top.PHP' due to insufficient sanitization of the '123' 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.	CJ LinkOut Cross-Site Scripting CAN-2005-2900	Medium	Secunia Advisory: SA16970, September 27, 2005
CJ Design CJ Tag Board 3.0	Cross-Site Scripting vulnerabilities have been reported in 'details.php' due to insufficient sanitization of the 'date,' 'time,' 'name,' 'ip,' and 'agent' parameters, and in 'display.php' due to insufficient sanitization of the 'msg' parameter, which could let a remote malicious user execute arbitrary	CJ Tag Board Multiple Cross-Site Scripting CAN-2005-2899	Medium	Secunia Advisory: SA16966, September 27, 2005

	HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.			
CJ Design CJ Web2Mail 3.0	Cross-Site Scripting vulnerabilities have been reported in 'thankyou.php' due to insufficient sanitization of the 'name,' 'message,' and 'ip' parameters and in 'web2mail.php' due to insufficient sanitization of the 'emsg' 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.	CJ Web2Mail Multiple Cross-Site Scripting CAN-2005-2901	Medium	Secunia Advisory: SA16963, September 27, 2005
CMS Made Simple CMS Made Simple 0.10	Several vulnerabilities have been reported: a vulnerability was reported in the 'admin/lang.php' script due to insufficient authentication, which could let a remote malicious user bypass authentication procedures; and a vulnerability was reported in 'admin/lang.php' due to insufficient verification of the 'nls[file][vx][vxsfx]' parameter, which could let a remote malicious user include arbitrary files. **Upgrade available at:** **http://cmsmadesimple.org/downloads/cmsmadesimple-0.10.2.tar.gz** There is no exploit code required; however, a Proof of Concept exploit has been published.	CMS Made Simple Authentication Bypass & File Include CAN-2005-2846	High	Secunia Advisory: SA16654, September 1, 2005 **Security Focus, Bugtraq ID: 14709, September 26, 2005**
CMS Made Simple CMS Made Simple 0.10	A Cross-Site Scripting vulnerability has been reported in 'index.php' 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; however, a Proof of Concept exploit has been published.	CMS Made Simple Cross-Site Scripting CAN-2005-3083	Medium	Security Focus, Bugtraq ID: 14937, September 26, 2005
contentServ contentServ 3.1	A vulnerability has been reported in 'admin/about.php' due to insufficient verification of the 'ctsWebsite' parameter before including files, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. An exploit script has been published.	ContentServ Local File Include CAN-2005-3086	Medium	Security Focus, Bugtraq ID: 14943, September 26, 2005

GeSHi GeSHi 1.0 .0-1.0.7.2	A Directory Traversal vulnerability has been reported in 'example.php' due to an input validation error, which could let a remote malicious user obtain sensitive information. Updates available at: http://sourceforge.net/project/showfiles.php?group_id=114997 There is no exploit code required.	GeSHI Directory Traversal CAN-2005-3080	Medium	Security Focus, Bugtraq ID: 14903, September 22, 2005
IBM Lotus Domino 6.5.4	A Cross-Site Scripting vulnerability has been reported due to insufficient validation of data supplied through URI parameters, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade information available at: http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg21201845 There is no exploit code required.	IBM Lotus Domino Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 14901, September 22, 2005
JPortal Web Portal JPortal Web Portal 2.3.1, 2.2.1	An SQL injection vulnerability has been reported in 'download.php' due to insufficient sanitization of user-supplied input, 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.	JPortal SQL Injection CAN-2005-3052	Medium	Security Focus, Bugtraq ID: 14926, September 23, 2005
Land Down Under Land Down Under 801	An SQL injection vulnerability has been reported due to insufficient sanitization of various scripts passed to the 'Referer' HTTP header, 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.	Land Down Under Remote SQL Injection	Medium	Secunia Advisory: SA16878, September 21, 2005
lucidCMS lucidCMS 1.0.11	A Cross-Site Scripting vulnerability has been reported in 'index.php' 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; however, a Proof of Concept exploit has been published.	LucidCMS Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 14951, September 27, 2005

Microsoft Internet Explorer Macintosh Edition 5.2.3	A remote Denial of Service vulnerability has been reported when Internet Explorer attempts to render a Web page with malformed content. No workaround or patch available at time of publishing. An exploit script has been published.	Microsoft Internet Explorer for Mac OS Remote Denial of Service CAN-2005-3077	Low	Security Focus, Bugtraq ID: 14899, September 22, 2005
Mozilla Firefox 1.0.6; Mozilla Browser 1.7.11, 1.7-1.7.9; **Thunderbird 1.0-1.0.6**	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/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-785.html** **http://rhn.redhat.com/errata/RHSA-2005-789.html** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/** **Mandriva:** **http://www.mandriva.com/security/advisories** **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.479350** 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 **Security Focus Bugtraq ID: 14888, September 22, 2005** **RedHat Security Advisories, RHSA-2005:785-9 & 789-11, September 22, 2005** **Ubuntu Security Notices, USN-USN-186-1 & 186-2, September 23 & 25, 2005** **US-CERT VU#914681** **Mandriva Linux Security Update Advisory, MDKSA-2005:169, September 26, 2005** **Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005** **Slackware Security Advisory, SSA:2005-269-01, September 26, 2005**
Mozilla.org Netscape 8.0.3.3, 7.2; Mozilla Firefox 1.5 Beta1, 1.0.6; Mozilla Browser 1.7.11; **Mozilla Thunderbird 1.0.6**	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:	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

	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 **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** A Proof of Concept exploit script has been published.		Advisory GLSA 200509-11, September 18, 2005 **Security Focus, Bugtraq ID: 14784, September 22, 2005** **Slackware Security Advisory, SSA:2005-269-01, September 26, 2005**

Multiple Vendors Mozilla Firefox 1.0-1.0.6; Mozilla Browser 1.7-1.7.11	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when processing malformed XBM images, which could let a remote malicious user execute arbitrary code; a vulnerability has been reported when unicode sequences contain 'zero-width non-joiner' characters, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported due to a flaw when making XMLHttp requests, which could let a remote malicious user spoof XMLHttpRequest headers; a vulnerability was reported because a remote malicious user can create specially crafted HTML that spoofs XML objects to create an XBL binding to execute arbitrary JavaScript with elevated (chrome) permissions; an integer overflow vulnerability was reported in the JavaScript engine, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because a remote malicious user can load privileged 'chrome' pages from an unprivileged 'about:' page, which could lead to unauthorized access; and a window spoofing vulnerability has been reported when a blank 'chrom' canvas is obtained by opening a window from a reference to a closed window, which could let a remote malicious user conduct phishing type attacks. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-789.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/ Mandriva: http://www.mandriva.com/security/advisories 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.479350	Mozilla Browser / Firefox Multiple Vulnerabilities CAN-2005-2701 CAN-2005-2702 CAN-2005-2703 CAN-2005-2704 CAN-2005-2705 CAN-2005-2706 CAN-2005-2707	High	Mozilla Foundation Security Advisory, 2005-58, September 22, 2005 RedHat Security Advisory, RHSA-2005:789-11, September 22, 2005 Ubuntu Security Notices, USN-186-1 & 186-2, September 23 & 25, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:169 & 170, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005

	Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Netscape Browser 8.0.3.3; Mozilla Firefox 1.0-1.0.6, Mozilla Browser 1.7-1.7.11	A remote Denial of Service vulnerability has been reported when a malicious user creates a Proxy Auto-Config (PAC) script that contains a specially crafted eval() statement. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ There is no exploit code required.	Multiple Browser Proxy Auto-Config Scripts Remote Denial of Service CAN-2005-3089	Low	Security Tracker Alert ID: 1014949, September 21, 2005
Multiple Vendors Gentoo Linux; Apache Software Foundation Apache 2.1-2.1.5, 2.0.35-2.0.54, 2.0.32, 2.0.28, Beta, 2.0 a9, 2.0	A remote Denial of Service vulnerability has been reported in the HTTP 'Range' header due to an error in the byte-range filter. Patches available at: http://issues.apache.org/bugzilla/attachment.cgi?id=16102 Gentoo: http://security.gentoo.org/glsa/glsa-200508-15.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Debian: http://security.debian.org/pool/updates/main/a/apache2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE **Avaya:** **http://support.avaya.com/**	Apache Remote Denial of Service CAN-2005-2728	Low	Secunia Advisory: SA16559, August 25, 2005 Security Advisory, GLSA 200508-15, August 25, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 Fedora Update Notifications, FEDORA-2005-848 & 849, September 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005 **Avaya Security Advisory, ASA-2005-204, September 23, 2005**

	elmodocs2/security/ ASA-2005-204.pdf There is no exploit code required.			
Multiple Vendors Mantis 0.19.0a-0.19.2, 0.18-0.18.3; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability has been reported in the 'mantis/view_all_set.php' script, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability has been reported in 'mantis/view_all_ bug_page.php' due to insufficient sanitization before returned to users, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input before used in and SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available for the first two vulnerabilities available at: http://www.mantisbt.org/ download.php Debian: http://security.debian.org/ pool/updates/main/ m/mantis/ **Gentoo:** **http://security.gentoo.org/ glsa/glsa-200509-16.xml** There is no exploit code required.	Mantis Multiple Input Validation CAN-2005-2556 CAN-2005-2557	Medium	Debian Security Advisory, DSA 778-1, August 19, 2005 Secunia Advisory: SA16506, August 22, 2005 **Gentoo Linux Security Advisory, GLSA 200509-16, September 24, 2005**

Multiple Vendors
PHPXMLRPC 1.1.1;
PEAR XML_RPC 1.3.3;
Drupal 4.6-4.6.2, 4.5- 4.5.4;
Nucleus CMS Nucleus CMS 3.21, 3.2, 3.1, 3.0, RC, 3.0.;
MailWatch for MailScanner 1.0.1;
eGroupWare 1.0.6, 1.0.3, 1.0.1, 1.0.0.007, 1.0
	A vulnerability has been reported in XML-RPC due to insufficient sanitization of certain XML tags that are nested in parsed documents being used in an 'eval()' call, which could let a remote malicious user execute arbitrary PHP code.
	PHPXMLRPC :
	http://prdownloads. sourceforge.net/ phpxmlrpc/xmlrpc. 1.2.tgz?download
	Pear:
	http://pear.php.net/ get/XML_RPC-1.4.0.tgz
	Drupal:
	http://drupal.org/files/ projects/drupal-4.5.5.tar.gz
	eGroupWare:
	http://prdownloads. sourceforge.net/ egroupware/
		PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution
		CAN-2005-2498
			High	Security Focus, Bugtraq ID 14560, August 15, 2995
				Security Focus, Bugtraq ID 14560, August 18, 2995
				RedHat Security Advisory, RHSA-2005:748-05, August 19, 2005
				Ubuntu Security Notice, USN-171-1, August 20, 2005
				Mandriva Linux Security Update Advisory, MDKSA-2005:146, August 22, 2005
				Gentoo Linux Security Advisory, GLSA 200508-13 & 14, & 200508-18,

	eGroupWare-1.0.0.009.tar .gz?download MailWatch: http://prdownloads.sourceforge.net/mailwatch/mailwatch-1.0.2.tar.gz Nucleus: http://prdownloads.sourceforge.net/nucleuscms/nucleus-xmlrpc-patch.zip ?download RedHat: http://rhn.redhat.com/errata/RHSA-2005-748.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200508-13.xml http://security.gentoo.org/glsa/glsa-200508-14.xml http://security.gentoo.org/glsa/glsa-200508-18.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/p/php4/ SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-20.xml http://security.gentoo.org/glsa/glsa-200508-21.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/p/phpgroupware/		August 24 & 26, 2005 Fedora Update Notifications, FEDORA-2005-809 & 810, August 25, 2005 Debian Security Advisory, DSA 789-1, August 29, 2005 SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005 Gentoo Linux Security Advisory, GLSA GLSA 200508-20& 200508-21, August 30 & 31, 2005 Slackware Security Advisory, SSA:2005-242-02, August 31, 2005 Debian Security Advisory, DSA 798-1, September 2, 2005 SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Slackware Security Advisories, SSA:2005-251-03 & 251-04, September 9, 2005 **Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005**

	SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/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-200509-19.xml** There is no exploit code required.			
MultiTheft Auto MultiTheftAuto 0.5 patch 1	Several vulnerabilities have been reported: a vulnerability has been reported in admin command 40 due to an authentication error, which could let a remote malicious user obtain unauthorized access; and a remote Denial of Service vulnerability has been reported in admin command 40 due to an error. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MultiTheftAuto Server Unauthorized Access & Remote Denial of Service CAN-2005-3064 CAN-2005-3065	Medium	Secunia Advisory: SA16926, September 26, 2005
my little homepage my little forum 1.5, 1.3	An SQL injection vulnerability has been reported in 'search.php' due to insufficient sanitization of user-supplied input, 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 script has been published.	My Little Forum SQL Injection CAN-2005-3045	Medium	Security Focus, Bugtraq ID: 14908, September 22, 2005
Nokia Nokia 7610, 3210	A remote Denial of Service vulnerability has been reported in Bluetooth OBEX transfers due to a failure to handle certain filename characters. No workaround or patch available at time of publishing. There is no exploit code required.	Nokia 3210 & 7610 Remote OBEX Denial of Service CAN-2005-3093	Low	Security Focus, Bugtraq ID: 14948, September 27, 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	Opera Mail Client Attachment Spoofing & Arbitrary JavaScript Execution	Medium	Secunia Advisory: SA16645, September 20, 2005 **SUSE Security Announcement,**

	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/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	CAN-2005-3006 CAN-2005-3007		**SUSE-SA:2005:057, September 26, 2005**
PHP Group PHP 5.0.5, 4.4.0	A vulnerability has been reported in the 'open_basedir' directive due to the way PHP handles it, 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.	PHP 'Open_BaseDir' Information Disclosure CAN-2005-3054	Medium	Security Focus, Bugtraq ID: 14957, September 27, 2005
phpMyFAQ Team phpMyFAQ 1.5.1	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in 'password.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; a Cross-Site vulnerability was reported in 'footer.php' due to insufficient sanitization of the 'PMF_CONF[version]' parameter and in 'header.php' due to insufficient sanitization of the 'PMF_LANG [metaLanguage]' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a Directory Traversal vulnerability was reported in 'index.php' which could let a remote malicious user obtain sensitive information; a vulnerability was reported in 'index.php' due to insufficient verification of the 'LANGCODE' parameter before including files, which could let a remote malicious user include arbitrary files or execute arbitrary PHP code; and a vulnerability was reported because log files are insecurely placed inside the web root, which could let a remote malicious user obtain sensitive information. Updates available at: http://www.phpmyfaq.de/download.php There is no exploit code required; however, Proof of Concept exploits have been published.	phpMyFAQ SQL Injection, Cross-Site Scripting, & Remote Command Execution CAN-2005-3046 CAN-2005-3047 CAN-2005-3048 CAN-2005-3049 CAN-2005-3050	High	Secunia Advisory: SA16933, September 26, 2005
Pierre Chifflier wzdftpd 0.5.4	A vulnerability has been reported due to insufficient sanitization of 'SITE' command parameters, which could let	Wzdftpd Remote Arbitrary Command	High	Security Focus, Bugtraq ID: 14935 , September 26, 2005

	a remote malicious user execute arbitrary commands. No workaround or patch available at time of publishing. An exploit has been published.	Execution CAN-2005-3081		
Polipo Polipo 0.9-0.9.8	A buffer overflow vulnerability has been reported due to an off-by-one error when NL-terminated headers are parsed, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Upgrades available at: http://www.pps.jussieu.fr/~jch/software/files/polipo/polipo-0.9.9.tar.gz Currently we are not aware of any exploits for this vulnerability.	Polipo Off-By-One Buffer Overflow	High	Security Focus, Bugtraq ID: 14961, September 28, 2005
PostNuke Development Team PostNuke Phoenix 0.760	A file include vulnerability has been reported in 'PN_BBCode' due to insufficient sanitization of user-supplied input, which could let a malicious user obtain unauthorized access. Upgrades available at: http://news.postnuke.com/Downloads-req-getit-lid-517.html There is no exploit code required.	PostNuke File Include	Medium	Security Focus, Bugtraq ID: 14958, September 28, 2005
PunBB PunBB 1.2.1-1.2.7	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'forgotten e-mail' feature, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the user language selection, which has an unknown impact. Upgrades available at: http://www.punbb.org/download/punbb-1.2.8.tar.gz There is no exploit code required.	PunBB Cross-Site Scripting & File Include CAN-2005-3078 CAN-2005-3079	Medium	Secunia Advisory: SA16908, September 22, 2005
Riverdark Studios RSS Syndicator module 2.1.7	Multiple Cross-Site Scripting vulnerabilities have been reported in 'rss.php' due to insufficient HTML filtering from 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; however, a Proof of Concept exploit has been published.	Riverdark RSS Syndicator Module Multiple Cross-Site Scripting CAN-2005-3085	Medium	Security Tracker Alert ID: 1014969, September 24, 2005
SEO-Board SEO-Board 1.0.2	An SQL injection vulnerability has been reported in 'admin.php' due to insufficient sanitization of the 'user_pass_sha1' parameter before	SEO-Board SQL Injection	Medium	Secunia Advisory: SA16949, September 26, 2005

	using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://seo-board.com/ seo-board103.zip There is no exploit code required.	CAN-2005-3082		
Simplog Simplog 0.9 .1	SQL injection vulnerabilities have been reported in 'archive.php' due to insufficient sanitization of the 'pid,' 'blogid,' 'cid,' and 'm' parameters and in 'blogadmin.php' due to insufficient sanitization of the 'blogid' parameter, which could let a remote malicious user execute arbitrary SQL code. The vendor has released version 0.9.2 beta 2 to address this issue. There is no exploit code required.	Simplog SQL Injection CAN-2005-3076	Medium	Secunia Advisory: SA16881, September 21, 2005
Six Apart Movable Type 3.17	Multiple vulnerabilities have been reported: a vulnerability was reported in the password reset functionality because different error messages are returned depending on whether or not a username exists, which could let a remote malicious user obtain sensitive information; a vulnerability was reported because files that contain arbitrary file extensions can be uploaded to a directory inside the web root; a Cross-Site Scripting vulnerability was reported when creating new blog entries due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'mt-comments.cgi' script because external URLs in comments are redirected, which could trick a user into visiting a malicious web site. Update available at: http://www.sixapart.com/ movabletype/ There is no exploit code required.	Movable Type Multiple Remote Vulnerabilities CAN-2005-3101 CAN-2005-3102 CAN-2005-3103 CAN-2005-3104	High	Secunia Advisory: SA16899, September 22, 2005
Sony PSP 2.0 firmware	A buffer overflow vulnerability has been reported in the TIFF library when processing a specially crafted TIFF image, which could let a remote malicious user cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Sony PSP TIFF Image Handling Remote Buffer Overflow CAN-2005-3084	Low	Secunia Advisory: SA16922, September 26, 2005
TWiki TWiki 20040903, 20040902, 20040901, 20030201	A vulnerability has been reported in the '%INCLUDE' variable due to insufficient sanitization of the 'rev' attribute before used in a shell expression, which could let a remote malicious user execute arbitrary code.	TWiki Remote Arbitrary Command Execution CAN-2005-3056	High	TWiki Security Advisory, September 28, 2005

	Patches available at: http://twiki.org/cgi-bin/view/Codev/UncoordinatedSecurityAlert23Feb2005 There is no exploit code required; however, a Proof of Concept exploit has been published.			
UNU Networks MailGust 1.9	An SQL injection vulnerability has been reported in the password functionality due to insufficient sanitization of the 'email' field 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 script has been published.	UNU Networks Mailgust SQL Injection CAN-2005-3063	Medium	Security Focus, Bugtraq ID: 14933, September 24, 2005
Zengaia Zengaia 0.1.5	An SQL injection vulnerability has been reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://www.mpc-donkey.de/zengaia/zengaia0.2.1src.zip There is no exploit code required.	Zengaia SQL Injection CAN-2005-3075	Medium	Secunia Advisory: SA16896, September 21, 2005

[back to top]

Wireless

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

- **Asia To Dominate WiMAX Market, Study Claims:** According to a study released by the market research firm, In-Stat, about 45 percent of all WiMAX subscribers in 2009 will be in the Asia Pacific region of the world. The study predicts that the number of subscribers in that region will increase from 80,000 this year to about 3.8 million in 2009. South Korea will be the most active in terms of WiMAX. Chinese operators will account for 34 percent of all equipment purchases and Japan will account for 17 percent, the study claims. Source: http://www.networkingpipeline.com/news/171201264.
- **Mobile Users Are Lax On Security: Survey:** According to a survey conducted by Bluefire Security Technologies, Inc. found that while most users are concerned about security, and while more than half their companies would invest more in mobile technology if these concerns were addressed, only 40% currently use mobile security tools. 44% of respondents said that, while they have concerns, neither they nor their companies have any immediate intentions to implement mobile security. Source: http://www.networkingpipeline.com/showArticle.jhtml?articleID=171200908.
- **New security proposed for do it all phones:** The Trusted Computing Group (TCG) which is backed by Nokia, Motorola, Intel, Samsung, VeriSign, and Vodafone plan to unveil a plan at a conference sponsored by the Cellular Telecommunications & Internet Association proposing new hardware-based security standards for mobile phones. The TCG has already developed similar specifications for PCs and servers. Source: http://news.com.com/New+security+proposed+for+do-it-all+phones/2100-1037_3-5883341.html?tag=nefd.lede.

Wireless Vulnerabilities

- **New Mobile Virus Also Aims At PCs:** According to F-Secure a new trojan, Cardtrap A, exists that is aimed at smartphones based on the Symbian platform also attempts to infect PCs. When the trojan attempts to infect the smartphone, it also copies two Windows worms to the phone's memory card. The two PC viruses are Win32/Padobot.Z and Win32/Rays. Source: http://informationweek.com/story/showArticle.jhtml?articleID=171100069 .
- **Nokia 3210 & 7610 Remote OBEX Denial of Service:** A remote Denial of Service vulnerability has been reported in Bluetooth OBEX transfers due to a failure to handle certain filename characters in Bluetooth OBEX transfers.

- **wlan_webauth.txt:** A script that redirects a wireless client to a fake a login page for a WLAN.
- **HijackHeadSet.tx:** An article titled, "Hijacking Bluetooth Headsets for Fun and Profit".

[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 Chronological Order)	Script name	Workaround or Patch Available	Script Description
September 28, 2005	kmalloc_exploitation.pdf	N/A	A whitepaper that describes kmalloc related kernel vulnerabilities and how to properly exploit them. Also includes a sample exploit.
September 28, 2005	wlan_webauth.txt	N/A	A script that redirects a wireless client to a fake a login page for a WLAN.
September 28, 2005	lucidCMS.txt	No	Exploitation details LucidCMS Cross-Site Scripting vulnerability.
September 28, 2005	mantis-poc.txt	Yes	An exploit script that scans remote databases for common logins and passwords.
September 27, 2005	imap4d_FreeBSD_exploit.c	Yes	Exploit for the GNU Mailutils Format String vulnerability.
September 26, 2005	xmlhttpRequestpaper.txt	N/A	Whitepaper entitled "Exploiting the XmlHttpRequest object in IE - Referrer spoofing, and a lot more."
September 26, 2005	contentServ.txt	No	Exploitation details for the ContentServ Local File Include vulnerability.
September 26, 2005	poppassd-freebsd.sh.txt poppassd-lnx.sh.txt	No	Proof of Concept exploits for the Qpopper Local Arbitrary File Modification vulnerability.
September 26, 2005	wzdftpdwarez.pl.txt	No	Exploit for the Wzdftpd Remote Arbitrary Command Execution vulnerability.
September 26, 2005	mtaboom.c mtaboom.zip	No	Proof of Concept exploit for the MultiTheftAuto Server Unauthorized Access & Remote Denial of Service vulnerability.
September 26, 2005	efriends.txt	No	Exploit details for the AlstraSoft E-Friends Remote File Include vulnerability.
September 26, 2005	helix4real.c OSG_Advisory_13.txt	Yes	Exploits the RealNetworks RealPlayer & Helix Player Format String vulnerability.
September 26, 2005	barracuda_img_exec.pl	Yes	Proof of Concept exploit for the Barracuda Spam Firewall Remote Code Execution vulnerability.
September 24, 2005	HijackHeadSet.txt	N/A	An article titled, "Hijacking Bluetooth Headsets for Fun and Profit".
September 24, 2005	jPortalSQL.txt	No	Exploitation details for the JPortal SQL Injection vulnerability.
September 24, 2005	mailgust_xpl.php maildisgust.txt	No	Proof of Concept exploit for the UNU Networks MailGust SQL Injection Vulnerability.

September 23, 2005	aim_jack.tar.gz	N/A	Two tools, aim-jack, a utility that allows a logged in AIM user to keep anyone else from signing on in another location, and aim_crack, which is a perl script used to conduct dictionary attacks against AIM hashed passwords.
September 23, 2005	mercury_imap.c	Yes	Script that exploits the Mercury Mail Multiple Remote IMAP Stack Buffer Overflow vulnerability.
September 23, 2005	phpmyfuck151.html	Yes	Exploitation details for the phpMyFAQ SQL Injection, Cross-Site Scripting, & Remote Command Execution vulnerabilities.
September 22, 2005	HYA-2005-008-alstrasoft-epay-pro.txt	No	Exploitation details for the EPay Pro Directory Traversal vulnerability.
September 22, 2005	dscribe14.txt	No	Exploitation details for the Digital Scribe SQL Injection vulnerability.
September 22, 2005	cutenxpl.php.txt	No	Exploit for the CuteNews Arbitrary PHP vulnerability.
September 22, 2005	mlfexpl.php mylittle15_16b.txt	No	Proof of Concept exploits for the My Little Forum SQL Injection vulnerability.
September 22, 2005	IE_Crash.html	No	Script that exploits the Microsoft Internet Explorer for Mac OS Remote Denial of Service
September 22, 2005	20050917-vbulletin-3.0.8.txt	Yes	Detailed exploitation for the vBulletin multiple SQL injection, cross site scripting, and arbitrary file upload vulnerabilities.
September 22, 2005	cirt-37-advisory.pdf	Yes	Exploitation details for the TAC Vista Directory Traversal vulnerability.

[back to top]

Trends

- **Password Overload Makes Enterprise Systems Less Secure:** According to a survey released by RSA Security, 28 percent of corporate workers juggle 13 or more passwords required to access Windows, specific applications, and Web portals. Another 30 percent have to deal with between 6 and 12 passwords. Source: http://www.techweb.com/wire/security/171201073;jsessionid=LQWK5KTXEH154QSNDBCSKH0CJUMEKJVN.
- **Name that worm plan looks to cut through chaos:** The U.S. Computer Emergency Readiness Team (US-CERT) plans to use the Common Malware Enumeration (CME) initiative identifiers for malicious code. Zotob.E, Tpbot-A, Rbot.CBQ, and IRCbot.worm were all names given to a single worm that wreaked havoc in Windows 2000 systems last month. Among the plethora of identifiers, perhaps the most useful CME-540 didn't make an impact. But that's about to change. Source: http://news.com.com/Name+that+worm--plan+looks+to+cut+through+chaos/2100-7349_3-5876293.html?tag=alert.
- **New Phish Deceives With Phony Certificates:** An Internet security vendor, SurfControl warns that a new advanced form a phishing dubbed "secured phishing" has surfaced. "Secured phishing' relies on self-signed digital certificates and can easily fool all but the most cautious consumers. Source: http://www.techweb.com/wire/security/171100298;jsessionid=JIA55XLPAW02YQSNDBGCKH0CJUMEKJVN.

[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 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 28, 2005

[back to top]

Last updated September 29, 2005