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

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

- blogBuddies Cross-Site Scripting
- BosDates SQL Injection
- **Cisco PIX Invalid TCP Checksum Remote Denial of Service (Updated)**
- **Cisco IPSec IKE Traffic Remote Denial of Service (Updated)**
- Cisco IOS HTTP Service HTML Injection
- Clavister Firewall and Security Gateway Denial of Service
- Comdev Vote Caster SQL Injection
- CommodityRentals SQL Injection
- Creative Digital Resources SocketKB SQL Injection & File Include
- DMANews SQL Injection
- DotClear Unspecified Trackback
- 1-2-3 Music Store SQL Injection
- edmoBBS SQL Injection
- eFiction Input Validation
- Entergal MX Multiple SQL Injection
- Enterprise Connector SQL Injection
- Fantastic Scripts Fantastic News SQL Injection
- FAQ System SQL Injection
- freeForum SQL Injection
- FreeWebStat Multiple Cross-Site Scripting
- GhostScripter Amazon Shop Cross-Site Scripting
- GuppY Remote File Include & Command Execution
- Helpdesk Issue Manager SQL Injection
- **Horde Error Message Cross-Site Scripting (Updated)**
- Horde MIME Viewers Script Insertion
- IPUpdate Remote Buffer Overflow
- IsolSoft Support Center SQL Injection
- Kadu Remote Denial of Service
- kPlaylist Search Cross-Site Scripting
- ltwCalendar SQL Injection
- **Macromedia Flash Array Index Remote Arbitrary Code Execution (Updated)**
- **Mambo Open Source Remote File Include (Updated)**
- **Multiple Vendors Inkscape SVG Image Buffer Overflow (Updated)**
- **Multiple Vendors Lynx URI Handlers Arbitrary Command Execution (Updated)**
- **phpSysInfo Multiple Vulnerabilities (Updated)**
- **Multiple Vendors PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution (Updated)**
- **Multiple Vendors PHP Group Exif Module Remote Denial of Service (Updated)**
- **Multiple Vendors Ethereal Multiple Protocol Dissector Vulnerabilities (Updated)**
- **Multiple Vendors XML-RPC for PHP Remote Code Injection (Updated)**
- N-13 News SQL Injection
- Nelogic Nephp Publisher SQL Injection
- Nicecoder iDesk SQL Injection
- Novell ZENworks Security Bypassing
- Athena PHP Website Administration Remote File Include
- Opera Web Browser JNI Routine Handling Remote Denial of Service
- Orbit Scripts SmartPPC Pro Cross-Site Scripting
- Orca Blog SQL Injection
- Orca Forum SQL Injection
- Orca Knowledgebase SQL Injection
- Orca Ringmaker SQL Injection
- OTRS SQL Injection & Cross-Site Scripting
- OvBB Multiple SQL Injection
- PBLang Bulletin Board System Multiple HTML Injection
- PDJK-support Suite Multiple SQL Injection
- PHP Doc System Local File Include
- **PHP 'Open_BaseDir' Information Disclosure (Updated)**
- **PHP Multiple Vulnerabilities (Updated)**
- PHP Upload Center Directory Traversal
- PHPAlbum File Include
- PHPGreetz Remote File Include
- PHP MB_Send_Mail Arbitrary Header Injection
- PHPPost Subject HTML Injection
- PHP Web Statistik Multiple Vulnerabilities
- PmWiki Cross-Site Scripting
- Q-News Remote File Include
- QNX Phgrafx Buffer Overflow
- Quality Unit Post Affiliate Pro SQL Injection & File Include
- Randshop SQL Injection
- Real Soft Studio UGroup SQL Injection
- AllWeb Search SQL Injection
- sCssBoard Cross-Site Scripting
- SearchSolutions Cross-Site Scripting
- Sensation Designs KBase Express Multiple SQL Injection
- Top Music Module SQL Injection

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 Attack Scripts	Common Name / CVE Reference	Risk	Source
ASP-Rider 1.6	A vulnerability has been reported in ASP-Rider that could let remote malicious users perform SQL injection. 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.	ASP-Rider SQL Injection CVE-2005-3931	Medium	Secunia, Advisory: SA17792, November 30, 2005
Freeftpd 1.0.10	Multiple vulnerabilities have been reported in Freeftpd that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Freeftpd Denial of Service CVE-2005-3812	Low	Security Focus , ID: 15557 , November 25, 2005
MailEnable Professional 1.7, Enterprise 1.1	A vulnerability has been reported in MailEnable that could let remote malicious users cause a Denial of Service. A vendor solution is available: http://www.mailenable.com/ hotfix/MEIMAPS.ZIP	MailEnable Denial of Service CVE-2005-3813	Low	Security Tracker, Alert ID: 1015268, November 24, 2005

	A Proof of Concept exploit has been published.			
Microsoft Internet Explorer	A vulnerability has been reported in Internet Explorer that could let remote malicious users to obtain unauthorized access. Vendor solutions available: http://www.microsoft.com/technet/security/advisory/911302.mspx **Updated to provide information on proof of concept code, malicious software, and provide additional references.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Internet Explorer Unauthorized Access CAN-2005-1790	Medium	Microsoft, Security Advisory 911302, November 21, 2005 USCERT, VU#887861 **Microsoft, Security Advisory 911302, November 29, 2005**
Microsoft Windows Microsoft Distribution Transaction Coordinator (MSDTC) and COM+	A buffer overflow vulnerability has been reported in Windows MSDTC and COM+ that could let local or remote malicious users execute arbitrary code, obtain elevated privileges or cause a Denial of Service. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-051.mspx Vendor has identified potential issues associated with fix: http://www.microsoft.com/technet/security/advisory/909444.mspx Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf Nortel: http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=366956&RenditionID= **An exploit has been published.**	Microsoft Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service CVE-2005-1978 CVE-2005-1979 CVE-2005-1980 CVE-2005-2119	High	Microsoft, Security Bulletin MS05-051, October 11, 2005 US-CERT VU#180868, US-CERT VU#950516 Technical Cyber Security Alert TA05-284A, October 11, 2005 Microsoft, Security Advisory 909444, October 14, 2005 Avaya, ASA-2005-214, October 11, 2005 Nortel, Security Advisory Bulletin 2005006316, November 11, 2005 **Security Focus, ID: 15056, November 27, 2005**
NetObjects Fusion 9	A vulnerability has been reported in NetObjects Fusion that could let remote malicious users disclose information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	NetObjects Fusion Information Disclosure CVE-2005-3923	Medium	Secunia, Advisory: SA17667, November 23, 2005
Online Tech Tools OASYS Lite 1.0	A vulnerability has been reported in OASYS Lite that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	OASYS Lite Cross-Site Scripting CVE-2005-3850	Medium	Security Focus, ID: 15605, November 28, 2005
Online Tech Tools OKBSYS Lite 1.0	A vulnerability has been reported in OKBSYS Lite that could let remote malicious users conduct Cross-Site scripting. No workaround or patch available at time of publishing. There is no exploit code required.	OKBSYS Lite Cross-Site Scripting CVE-2005-3851	Medium	Security Focus, ID: 15607, November 28, 2005
Panda Software WebAdmin, TruPrevent Personal 2006, 2005, Titanium 2006 Antivirus + Antispyware, Titanium 2005 Antivirus, Titanium Panda Security 3.0, Platinum 2006 Internet Security, EnterpriSecure Antivirus, ISA Secure, GateDefender, FileSecure with TruPrevent	A heap overflow vulnerability has been reported when attempting to decompress ZOO archive files, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Panda Software Antivirus Library ZOO Archive Heap Overflow CVE-2005-3922	High	Security Focus, Bugtraq ID: 15616, November 29, 2005

Technologies, FileSecure, ExchangeSecure, EnterpriSecure with TruPrevent Technologies, ClientShield with TruPrevent Technologies, BusinesSecure Antivirus, Antivirus Platinum 2.0, Antivirus for NetWare 2.0, ActiveScan 5.0				
SpeedProject SpeedCommander 10.51, 11, Squeez 5.0, ZipStar 5.0	Multiple buffer overflow vulnerabilities have been reported in SpeedCommander, Squeez, and ZipStar that could let remote malicious users execute arbitrary code. Upgrade to newest version: http://www.speedproject.de/enu/download.html Currently we are not aware of any exploits for this vulnerability.	SpeedProject Arbitrary Code Execution CVE-2005-3831 CVE-2005-3832	High	Secunia, Advisory: SA17420, November 24, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Apple Macintosh OS X	Multiple vulnerabilities have been reported: a vulnerability was reported when handling HTTP headers in the Apache 2 web server due to an error, which could let a remote malicious user conduct HTTP request smuggling attacks; a vulnerability was reported in the Apache web server's 'mod_ssl' module due to an error, which could let a remote malicious user bypass security restrictions; a vulnerability was reported in 'CoreFoundation' when resolving certain URLs due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in curl when handling NTML authentication due to an error, which could let a remote malicious user compromise a user's system; a vulnerability was reported in 'iodbcadmintoo,' which could let a malicious user execute arbitrary commands with elevated privileges; a vulnerability was reported in OpenSSL when handling certain compatibility options due to an error, which could let a remote malicious user perform rollback attacks; a vulnerability was reported in 'passwordserver' when handling the creation of an Open Directory master server due to an error, which could let a malicious user obtain sensitive information; a vulnerability was reported in the PCRE library used by Safari's JavaScript due to an integer overflow error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in Safari when a downloaded file that contains an overly long filename is downloaded, which could let a remote malicious user save the file outside the designated directory; a vulnerability was reported in Safari because JavaScript dialog boxes don't indicate the web site that created them, which could let a remote malicious user spoof dialog boxes; a vulnerability was reported in Webkit when handling specially crafted content due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in 'sudo' due to an error, which could let a malicious user execute arbitrary code; and a vulnerability was reported in the syslog server due to insufficient sanitization of messages before recording them, which could let a remote malicious user forge log entries and mislead the system administrator. Patch information available at: http://docs.info.apple.com/article.html?artnum=302847 Currently we are not aware of any exploits for these vulnerabilities.	Mac OS X Security Update CVE-2005-1993 CVE-2005-2088 CVE-2005-2491 CVE-2005-2700 CVE-2005-2757 CVE-2005-2969 CVE-2005-3185 CVE-2005-3700 CVE-2005-3701 CVE-2005-3702 CVE-2005-3703 CVE-2005-3704 CVE-2005-3705	High	Apple Security Update, APPLE-SA-2005-11-29, November 29, 2005
Centericq Centericq 4.20	A remote Denial of Service vulnerability has been reported when handling malformed packets on the listening port for ICQ messages. Debian: http://security.debian.org/pool/updates/main/c/centericq/ A Proof of Concept exploit script has been published.	Centericq Empty Packet Remote Denial of Service CVE-2005-3694	Low	Debian Security Advisory. DSA 912-1, November 30, 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 **SCO:** **ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.51** A Proof of Concept exploit has been published.	CUPS HTTP GET Denial of Service CVE-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 **SCO Security Advisory, SCOSA-2005.51, November 24, 2005**
Ezyhelp desk	Multiple vulnerabilities have been reported in Ezyhelpdesk that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Ezyhelpdesk SQL Injection CVE-2005-3826	Medium	Secunia, Advisory: SA17697, November 23, 2005
FAD Solutions DRZES HMS 3.2	Several vulnerabilities have been reported: an SQL injection vulnerability has been reported in some input passed in the customer interface due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability has been reported in 'register_domain.php' due to insufficient sanitization of the 'sld' parameter before returning to the user, 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.	drzes HMS SQL Injection & Cross-Site Scripting	Medium	Secunia Advisory: SA17755, November 29, 2005
GNU shtool 2.0.1 & prior	A vulnerability has been reported that could let a local malicious user gain escalated privileges. The vulnerability is caused due to temporary files being created insecurely. Gentoo: http://security.gentoo.org/glsa/glsa-200506-08.xml OpenPKG: ftp://ftp.openpkg.org/release/2.3 RedHat: http://rhn.redhat.com/errata/RHSA-2005-564.html Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: http://www.sgi.com/support/security/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Debian: http://security.debian.org/pool/updates/main/p/php4/ **Updates available at:** **http://www.php.net/get/php-4.4.0.tar.bz2/from/a/mirror** There is no exploit code required.	GNU shtool Insecure Temporary File Creation CVE-2005-1751	Medium	Secunia Advisory, SA15496, May 25, 2005 Gentoo Linux Security Advisory, GLSA 200506 -08, June 11, 200 OpenPKG Security Advisory, OpenPKG-SA-2005.011, June 23, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005 SGI Security Advisory, 20050703-01-U, July 15, 2005 Ubuntu Security Notice, USN-171-1, August 20, 2005 Debian Security Advisory, DSA 789-1, August 29, 2005 **Security Focus, Bugtraq ID: 13767, November 25, 2005**

Hewlett Packard Company HP-UX B.11.23, B.11.11, B.11.00	A vulnerability has been reported in HP UX running xterm, which could let a malicious user obtain unauthorized access. **Update 1: Preliminary xterm files are available.** Currently we are not aware of any exploits for this vulnerability.	HP-UX XTerm Unauthorized Access CVE-2005-3779	Medium	HP Security Advisory, HPSBUX02075, November 14, 2005 **HP Security Advisory, HPSBUX02075 Update 1, November 22, 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 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/u/unzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/u/unzip/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.	Info-ZIP UnZip File Permission Modification CVE-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 Ubuntu Security Notice, USN-191-1, September 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0053, September 30, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:197, October 26, 2005 Debian Security Advisory, DSA 903-1, November 21, 2005 **Conectiva Linux Announcement, CLSA-2005:1049, November 21, 2005**
Jed Wing CHM lib 0.36, 0.35, 0.3-0.33, 0.2, 0.1	A buffer overflow vulnerability has been reported in the '_chm_decompress_block()' function due to a boundary error when reading input, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://morte.jedrea.com/~jedwin/projects/chmlib/chmlib-0.37.tgz SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/c/chmlib/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200511-23.xml** Currently we are not aware of any exploits for this vulnerability.	CHM Lib Remote Buffer Overflow CVE-2005-3318	High	Security Focus, Bugtraq ID: 15211, October 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Debian Security Advisory, DSA 886-1, November 7, 2005 **Gentoo Linux Security Advisory, GLSA 200511-23, November 28, 2005**
Multiple Vendors ktools 0.3; Centericq 4.21, 4.20	A buffer overflow vulnerability has been reported in the 'VGETSTRING()' marco when generating the output string using the "vsprintf()" function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	KTools Remote Buffer Overflow CVE-2005-3863	High	Zone-H Research Center Security Advisory 200503, November 27, 2005
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc,	A vulnerability has been reported in the network bridging functionality, which could let a remote malicious user poison the bridge forwarding table. Upgrades available at:	Linux Kernel Network Bridge Information Disclosure	Medium	Security Focus, Bugtraq ID: 15536, November 22, 2005 Ubuntu Security Notice,

ia64, ia32; Linux kernel 2.6-2.6.12, 2.5.0-2.5.69, 2.4-2.4.32	http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.11.12.tar.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ There is no exploit code required.	CVE-2005-3272		USN-219-1, November 22, 2005

Multiple Vendors
Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;
TouchTunes Rhapsody, TouchTunes Maestro;
SuSE UnitedLinux 1.0, Novell Linux Desktop 9.0, Linux Professional 10.0 OSS, 10.0, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Personal 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Enterprise Server 9, 8, Linux Desktop 1.0;
RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, 2.1 IA64, 2.1, AS 4, AS 3, AS 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1;
GTK+ 2.8.6, 2.6.4, 2.4.14, 2.4.13, 2.4.10, 2.4.9, 2.4.1, 2.2.4, 2.2.3;
GNOME GdkPixbuf 0.22;
Gentoo Linux ;
Ardour 0.99
	Multiple vulnerabilities have been reported: an integer overflow vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' due to the insufficient validation of the 'n_col' value before using to allocate memory, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' when processing an XPM file that contains a large number of colors; and an integer overflow vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' when performing calculations using the height, width, and colors of a XPM file, which could let a remote malicious user execute arbitrary code or cause a Denial of Service.
	Updates available at:
	ftp://ftp.gtk.org/pub/gtk/v2.8/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-810.html
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200511-14.xml
	SuSE:
	ftp://ftp.suse.com/pub/suse/
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/g/gdk-pixbuf/
	Mandriva:
	http://www.mandriva.com/security/advisories
	Trustix:
	http://http.trustix.org/pub/trustix/
	Avaya:
	http://support.avaya.com/elmodocs2/security/ASA-2005-229.pdf
	Debian:
	http://security.debian.org/pool/updates/main/g/gtk+2.0/
	SGI:
	ftp://patches.sgi.com/support/free/security/advisories/
	Currently we are not aware of any exploits for these vulnerabilities.
		GTK+ GdkPixbuf XPM Image Rendering Library
		CVE-2005-2975
		CVE-2005-2976
		CVE-2005-3186
			High	Fedora Update Notifications FEDORA-2005-1085 & 1086, November 15, 2005
				RedHat Security Advisory, RHSA-2005:810-9, November 15, 2005
				Gentoo Linux Security Advisory GLSA 200511-14, November 16, 2005
				SUSE Security Announcement, SUSE-SA:2005:065, November 16, 2005
				Ubuntu Security Notice, USN-216-1, November 16, 2005
				Mandriva Linux Security Advisory, MDKSA-2005:214, November 18, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0066, November 22, 2005
				Avaya Security Advisory, ASA-2005-229, November 21, 2005
				Debian Security Advisory, DSA 911-1, November 29, 2005
				SGI Security Advisory, 20051101-01-U, November 29, 2005

Multiple Vendors Gentoo Linux; eix 0.5 .0-beta, 0.3 .0-r1	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user obtain sensitive information or cause a Denial of Service. Gentoo: http://security.gentoo.org/glsa/glsa-200511-19.xml	EIX Insecure Temporary File Creation CVE-2005-3785	Medium	Gentoo Linux Security Advisory, GLSA 200511-19, November 22, 2005

	There is no exploit code required.			
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/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-659.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-673.html http://rhn.redhat.com/errata/RHSA-2005-709.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-222.pdf Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for these vulnerabilities.	GDB Multiple Vulnerabilities CVE-2005-1704 CVE-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 RedHat Security Advisory, RHSA-2005:673-5 & RHSA-2005:709-6, October 5, 2005 Avaya Security Advisory, ASA-2005-222, October 18, 2005 Fedora Update Notifications, FEDORA-2005-1032 & 1033, October 27, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:215, November 23, 2005**
Multiple Vendors IPsec-Tools IPsec-Tools 0.5; KAME Racoon prior to 20050307	A remote Denial of Service vulnerability has been reported when parsing ISAKMP headers. Upgrades available at: http://www.kame.net/snap-users/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-232.html Gentoo: http://security.gentoo.org/	KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service CVE-2005-0398	Low	Fedora Update Notifications, FEDORA-2005-216 & 217, March 14, 2005 RedHat Security Advisory, RHSA-2005:232-10, March 23, 2005 Gentoo Linux Security Advisory, GLSA 200503-33, March 25, 2005 ALTLinux Security

	glsa/glsa-200503-30.xml ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/ipsec-tools/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.37 **SCO:** **ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.52** Currently we are not aware of any exploits for this vulnerability.			Advisory, March 29, 2005 SUSE Security Announcement, SUSE-SA:2005:020, March 31, 2005 Ubuntu Security Notice, USN-107-1, April 05, 2005 SCO Security Advisory, SCOSA-2005.37, September 9, 2005 **SCO Security Advisory, SCOSA-2005.52, November 28, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12, 2.4-2.4.31	A remote Denial of Service vulnerability has been reported due to a design error in the kernel. The vendor has released versions 2.6.13 and 2.4.32-rc1 of the kernel to address this issue. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Remote Denial of Service CVE-2005-3275	Low	Ubuntu Security Notice, USN-219-1, November 22, 2005
Multiple Vendors Linux kernel 2.6-2.6.14	A Denial of Service vulnerability has been reported in 'ptrace.c' when 'CLONE_THREAD' is used due to a missing check of the thread's group ID when trying to determine whether the process is attempting to attach to itself. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.2.tar.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PTrace 'CLONE_THREAD' Denial of Service CVE-2005-3783	Low	Secunia Advisory: SA17761, November 29, 2005 Fedora Update Notification, FEDORA-2005-1104, November 28, 2005
Multiple Vendors Linux kernel 2.6-2.6.15	A Denial of Service vulnerability has been reported in the 'time_out_leases()' function because 'printk()' can consume large amounts of kernel log space. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.15-rc3.bz2 An exploit script has been published.	Linux Kernel PrintK Local Denial of Service CVE-2005-3857	Low	Security Focus, Bugtraq ID: 15627, November 29, 2005
Multiple Vendors Linux kernel 2.6-2.6.15	A Denial of Service vulnerability has been reported because processes are improperly auto-reaped when they are being ptraced. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.15-rc3.bz2 Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PTraced Denial of Service CVE-2005-3784	Low	Security Focus, Bugtraq ID: 15625, November 29, 2005
Multiple Vendors MandrakeSoft Multi Network Firewall 2.0, Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2, Corporate Server 3.0 x86_64, 3.0;	A buffer overflow vulnerability has been reported due to insufficient validation of user-supplied NTLM user name data, which could let a remote malicious user execute arbitrary code. WGet: http://ftp.gnu.org/pub/gnu/wget/wget-1.10.2.tar.gz Daniel Stenberg:	Multiple Vendor WGet/Curl NTLM Username Buffer Overflow CVE-2005-3185	High	Security Tracker Alert ID: 1015056, October 13, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:182 & 183, October 13, 200 Ubuntu Security Notice,

GNU wget 1.10; Daniel Stenberg curl 7.14.1, 7.13.1, 7.13, 7.12.1-7.12.3, 7.11-7.11.2, 7.10.6-7.10.8	http://curl.haxx.se/libcurl-ntlmbuf.patch Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/curl/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200510-19.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-807.html http://rhn.redhat.com/errata/RHSA-2005-812.html SUSE: ftp://ftp.suse.com/pub/suse/ Slackware: ftp://ftp.slackware.com/pub/slackware/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for this vulnerability.			USN-205-1, October 14, 2005 Fedora Update Notifications FEDORA-2005-995 & 996, October 17, 2005 Fedora Update Notification, FEDORA-2005-1000, October 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 Gentoo Linux Security Advisory. GLSA 200510-19, October 22, 2005 RedHat Security Advisories, RHSA-2005:807-6 & RHSA-2005:812-5, November 2, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Slackware Security Advisory, SSA:2005-310-01, November 7, 2005 **Conectiva Linux Announcement, CLSA-2005:1045, November 21, 2005** **SGI Security Advisory, 20051101-01-U, November 29, 2005**
Multiple Vendors Miklos Szeredi FUSE 2.4 .0, 2.3.0, 2.3 -rc1, 2.2.1, 2.2; Gentoo Linux	A vulnerability has been reported because fusermount fails to securely handle special characters specified in mount points, which could let a malicious user cause a Denial of Service or add arbitrary mount points. Gentoo: http://security.gentoo.org/glsa/glsa-200511-17.xml **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	FUSE Mount Options Corruption CVE-2005-3531	Medium	Gentoo Linux Security Advisory, GLSA 200511-17, November 22, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:216, November 24, 2005**
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, WS 2.1, IA64, ES 4, ES 3, ES 2.1, IA64, AS 4, AS 3, 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; libungif libungif 4.1.3,	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported due to a NULL pointer dereferencing error; and a vulnerability was reported due to a boundary error that causes an out-of-bounds memory access, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=102202 Fedora: http://download.fedora.	Multiple Vendors libungif GIF File Handling CVE-2005-2974 CVE-2005-3350	High	Security Tracker Alert ID: 1015149, November 3, 2005 Fedora Update Notifications, FEDORA-2005-1045 & 1046, November 3, 2005 Gentoo Linux Security Advisory GLSA 200511-03, November 4, 2005

4.1, giflib 4.1.3; Gentoo Linux	redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-03.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-828.html SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libu/libungif4/ Debian: http://security.debian.org/pool/updates/main/libu/libungif4/ Mandriva: http://www.mandriva.com/security/advisories **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for these vulnerabilities.			RedHat Security Advisory, RHSA-2005:828-17, November 3, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Ubuntu Security Notice, USN-214-1, November 07, 2005 Debian Security Advisory, DSA 890-1, November 9, 2005 Mandriva Linux Security Advisory, MDKSA-2005:207, November 10, 2005 **SGI Security Advisory, 20051101-01-U, November 29, 2005**
Multiple Vendors Ubuntu Linux 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.8	A Denial of Service vulnerability has been reported due to a resource leak when handling POSIX timers in the 'exec()' function. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.9.tar.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Resource Leak Denial of Service CVE-2005-3271	Low	Ubuntu Security Notice, USN-219-1, November 22, 2005
Multiple Vendors Webmin 0.88 -1.230, 0.85, 0.76-0.80, 0.51, 0.42, 0.41, 0.31, 0.22, 0.21, 0.8.5 Red Hat, 0.8.4, 0.8.3, 0.1-0.7; Usermin 1.160, 1.150, 1.140, 1.130, 1.120, 1.110, 1.0, 0.9-0.99, 0.4-0.8; Larry Wall Perl 5.8.3-5.8.7, 5.8.1, 5.8 .0-88.3, 5.8, 5.6.1, 5.6, 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03	A format string vulnerability has been reported in the 'miniserv.pl' script due to a failure to properly handle format specifiers in formatted printing functions, which could let a remote malicious user cause a Denial of Service. No workaround or patch available at time of publishing. An exploit has been published.	Perl 'miniserv.pl' script Format String CVE-2005-3912	Low	Security Focus, Bugtraq ID: 15629, November 29, 2005
Net-SNMP Net-SNMP 5.2.1, 5.2, 5.1-5.1.2, 5.0.3 -5.0.9, 5.0.1	A remote Denial of Service vulnerability has been reported when handling stream-based protocols. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=12694&package_id =11571&release_id=338899	Net-SNMP Protocol Denial of Service CVE-2005-2177	Low	Secunia Advisory: SA15930, July 6, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Fedora Update Notifications,

	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-2005-720.html Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/net-snmp/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-395.html Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-225.pdf SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/n/net-snmp/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/u/ucd-snmp **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.			FEDORA-2005-561 & 562, July 13, 2005 RedHat Security Advisory, RHSA-2005:720-04, August 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:137, August 11, 2005 Ubuntu Security Notice, USN-190-1, September 29, 2005 RedHat Security Advisory, RHSA-2005:395-18, October 5, 2005 Conectiva Linux Announcement, CLSA-2005:1032, October 13, 2005 Avaya Security Advisory, ASA-2005-225, October 18, 200 SUSE Security Summary Report, Announcement ID: SUSE-SR:2005:024, October 21, 2005 Debian Security Advisory, DSA 873-1, October 26, 2005 Ubuntu Security Notice, USN-190-2, November 21, 2005 **Conectiva Linux Announcement, CLSA-2005:1050, November 21, 2005**
NuFW NuFW 1.1, 1.0.11-1.0.15	A Denial of Service vulnerability has been reported due to an error in packet parsing. Upgrades available at: http://nufw.org/download/nufw/nufw-1.0.16.tar.bz2 Currently we are not aware of any exploits for this vulnerability.	NuFW Malformed Packet Remote Denial of Service CVE-2005-3950	Low	Security Focus, Bugtraq ID: 15645, November 29, 2005
Omnistar Interactive Omnistar Live prior to 5.2	A vulnerability has been reported in Omnistar Live that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Omnistar Live SQL Injection CVE-2005-3840	Medium	Security Focus, ID: 15550, November 23, 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.	PCRE Regular Expression Heap Overflow CVE-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices,

	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.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/ Conectiva: ftp://atualizacoes.conectiva.com.br/		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 Announcement, CLSA-2005:1009, September 13, 2005 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 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 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005 Turbolinux Security Advisory, TLSA-2005-92, October 3, 2005 Avaya Security Advisory, ASA-2005-216, October 18, 2005

	10/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-216.pdf Trustix: http://http.trustix.org/pub/trustix/updates/ HP: http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE Trustix: http://http.trustix.org/pub/trustix/updates/ **Updated available at:** **http://www.php.net/get/php-5.1.0.tar.bz2/from/a/mirror** Currently we are not aware of any exploits for this vulnerability.			Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 HP Security Bulletin, HPSBUX02074, November 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0062, November 22, 2005 **Security Focus, Bugtraq ID: 14620, November 25, 2005**
PHP Labs Survey Wizard	An SQL injection vulnerability has been reported in 'survey.php' due to insufficient sanitization of the 'sid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP Labs Survey Wizard SQL Injection CVE-2005-3951	Medium	Secunia Advisory: SA17686, November 23, 2005
PHP Labs Top Auction	SQL injection vulnerabilities have been reported in 'viewcat.php' due to insufficient sanitization of the 'category' and 'type' parameters and insufficient sanitization of some parameters when performing a search, 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.	PHP Labs Top Auction Multiple SQL Injection CVE-2005-3952	Medium	Secunia Advisory: SA17687, November 23, 2005
Squid Squid 2.x	A remote Denial of Service vulnerability has been reported when handling certain FTP server responses. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE11-rfc1738_do_escape.patch Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.44 SUSE: ftp://ftp.suse.com	Squid FTP Server Response Handling Remote Denial of Service CVE-2005-3258	Low	Secunia Advisory: SA17271, October 20, 2005 Fedora Update Notifications, FEDORA-2005-1009 & 1010, October 20, 2005 Mandriva Linux Security Advisory, MDKSA-2005:195, October 26, 2005 SCO Security Advisory, SCOSA-2005.44, November 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Security Focus, Bugtraq ID: 15157, November 10, 2005 SUSE Security Summary Report, SUSE-SR:2005:027,

	/pub/suse/ IPCop: http://prdownloads.sourceforge.net/ipcop/ipcop-sources-1.4.10.tgz?download **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.			November 18, 2005 **Conectiva Linux Announcement, CLSA-2005:1047, November 21, 2005**
Sun Micro-systems, Inc. Solaris 10.0	Multiple buffer overflow vulnerabilities have been reported when handling excessive data supplied through command line arguments, which could let a malicious user execute arbitrary code. **Vendor solution available:** **http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102060-1** **An exploit script has been published.**	Sun Solaris Traceroute Multiple Buffer Overflows CVE-2005-2071	High	Security Focus, 14049, June 24, 2005 **Sun, Alert ID: 102060, November 23, 2005**
Sylpheed Sylpheed 2.0-2.0.3, 1.0.0-1.0.5	A buffer overflow vulnerability has been reported in 'ldif.c' due to a boundary error in the 'ldif_ get_line()' function when importing a LDIF file into the address book, which could let a remote malicious user obtain unauthorized access. Upgrades available at: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.6.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-13.xml Debian: http://security.debian.org/pool/updates/main/s/sylpheed/ **Debian:** **http://security.debian.org/pool/updates/main/s/sylpheed-claws/** **Currently we are not aware of any exploits for this vulnerability.**	Sylpheed LDIF Import Buffer Overflow CVE-2005-3354	Medium	Bugtraq ID: 15363, November 9, 2005 Fedora Update Notification, FEDORA-2005-1063, November 9, 2005 Gentoo Linux Security Advisory, GLSA 200511-13, November 15, 2005 Debian Security Advisory, DSA 906-1, November 22, 2005 **Debian Security Advisory, DSA 908-1, November 23, 2005**
T & D Systems ADC2000 NG Pro 1.2	An SQL injection vulnerability has been reported in 'adcbrowres.php' due to insufficient sanitization of the 'cat' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Proof of Concept exploits have been published.	ADC2000 NG Pro SQL Injection CVE-2005-3876	Medium	Secunia Advisory: SA17744, November 28, 2005
Tunez Tunez 1.21	Several vulnerabilities have been reported: an SQL injection vulnerability has been reported in 'songinfo.php' due to insufficient sanitization of the 'song_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'searchFor' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Tunez SQL Injection & Cross-Site Scripting CVE-2005-3833 CVE-2005-3834	Medium	Secunia Advisory: SA17692, November 23, 2005

unalz unalz 0.52, 0.51, 0.31, 0.23, 0.22, 0.2-0.5	A buffer overflow vulnerability has been reported when handling the '.alz' archive due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: (zip file) http://www.kipple.pe.kr/win/unalz/unalz-0.53.tgz An exploit script has been published.	Unalz Archive Filename Buffer Overflow CVE-2005-3862	High	Security Focus, Bugtraq ID: 15577, November 28, 2005
University of Washington UW-imapd imap-2004c1	A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version imap-2004g: ftp://ftp.cac.washington.edu/imap/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/u/uw-imap/ Gentoo: http://security.gentoo.org/glsa/glsa-200510-10.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandriva: http://www.mandriva.com/ security/advisories Slackware: ftp://ftp.slackware.com/pub/slackware/ **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.	UW-imapd Denial of Service and Arbitrary Code Execution CVE-2005-2933	High	Secunia, Advisory: SA17062, October 5, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005 Debian Security Advisory, DSA 861-1, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005 US-CERT VU#933601 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:189 & 194, October 21 & 26, 2005 Slackware Security Advisory, SSA:2005-310-06, November 7, 2005 **Conectiva Linux Announcement, CLSA-2005:1046, November 21, 2005**
Virtual Hosting Control System Virtual Hosting Control System (VHCS) 2.4.6.2, 2.2	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'vhcs/gui/errordocs/index.php' error page due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the domain alias management due to an unspecified error, which could let a remote malicious user hijack other users' forwards. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	VHCS Error Page Cross-Site Scripting & Domain Forward Hijack CVE-2005-3902 CVE-2005-3913	Medium	Secunia Advisory: SA17704, November 23, 2005
Zope Zope 2.6-2.8.1	A vulnerability has been reported in 'docutils' due to an unspecified error and affects all instances which exposes 'Restructured Text' functionality via the web. The impact was not specified. Hotfix available at: http://www.zope.org/Products/Zope/Hotfix 2005-10-09/security_alert/Hot fix_2005-10-09.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200510-20.xml SUSE: ftp://ftp.suse.com/pub/suse/	Zope 'Restructured Text' Unspecified Security Vulnerability CVE-2005-3323	Not Specified	Zope Security Alert, October 12, 2005 Gentoo Linux Security Advisory, GLSA 200510-20, October 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 **Debian Security Advisory, DSA 910-1, November 24, 2005**

	Debian: **http://security.debian.org/pool/updates/main/z/zope2.7/** Currently we are not aware of any exploits for this vulnerability.			

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
AFFCommerce Shopping Cart AFFCommerce Shopping Cart 1.1.4	SQL injection vulnerabilities have been reported in 'SubCategory.php' due to insufficient sanitization of the 'cl' parameter and in 'ItemInfo.php' and 'ItemReview.php' due to insufficient sanitization of the 'item_id' parameter, 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, Proof of Concept exploits have been published.	AFFCommerce Shopping Cart Multiple SQL Injection CVE-2005-3914	Medium	Secunia Advisory: SA17690, November 23, 2005
Agileco AgileBill 1.4.92	An SQL injection vulnerability has been reported in 'Product_Cat' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AgileBill Pro SQL Injection CVE-2005-3827	Medium	Security Tracker Alert ID: 1015272, November 25, 2005
Babe Logger Babe Logger V2	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'gal' parameter and in 'comments.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Babe Logger SQL Injection CVE-2005-3920	Medium	Security Focus, Bugtraq ID: 15580, November 28, 2005
BakBone NetVault 7.1	A vulnerability has been reported because 'vstatsmngr.exe' can be manipulated to obtain elevated privileges. **The vendor has released upgrades to address this issue. Please contact the vendor to obtain fixes.** An exploit script has been published.	BakBone NetVault 'NVStats Mngr.EXE' Elevated Privileges CVE-2005-1372	Medium	Security Focus, 13408, April 27, 2005 **Security Focus, Bugtraq ID:13408, November 25, 2005**
BASE Basic Analysis and Security Engine BASE Basic Analysis and Security Engine 1.2	An SQL injection vulnerability has been reported in 'base_qry_main.php' due to insufficient sanitization of the 'sig[1] parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Debian: http://security.debian.org/pool/updates/main/a/acidlab/ **Upgrades available at:** **http://prdownloads.sourceforge.net/secureideas/base-1.2.1.tar.gz?download** There is no exploit code required; however, a Proof of Concept exploit has been published.	Basic Analysis and Security Engine SQL Injection CVE-2005-3325	Medium	Secunia Advisory: SA17314, October 25, 2005 Debian Security Advisory DSA 893-1, November 14, 2005 **Security Focus, Bugtraq ID: 15199, November 30, 2005**
Bedeng PSP Bedeng PSP 1.1	SQL injection vulnerabilities have been reported in 'index.php' and 'download.php' due to insufficient sanitization of the 'cwhere' parameter and in 'baca.php' due to insufficient sanitization of the 'ckode'; parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Proof of Concept exploits have been published.	Bedeng PSP SQL Injection CVE-2005-3953	Medium	Security Focus, Bugtraq ID: 15583, November 28, 2005

BerliOS SourceWell 1.1.3	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'cnt' '' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	BerliOS SourceWell SQL Injection CVE-2005-3864	Medium	Security Focus, Bugtraq ID: 15586, November 28, 2005
blogBuddies 0.3	A vulnerability has been reported in blogBuddies that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	blogBuddies Cross-Site Scripting CVE-2005-3954 CVE-2005-3955	Medium	Security Focus, ID: 15555, November 24, 2005
BosDev BosDates 4.0	SQL injection vulnerabilities have been reported in 'calendar.php' due to insufficient sanitization of the 'year' and 'category' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	BosDates SQL Injection CVE-2005-3911	Medium	Secunia Advisory: SA17752, November 30, 2005
Cisco Systems Cisco PIX/ASA 7.0.1.4, 7.0, PIX OS, PIX Firewall 535, 525 6.3, 525, 520, 515E, 515, 506, 501, 6.3.3 (133), 6.3.2, 6.3.1, 6.3 (5), 6.3 (3.109), 6.3 (3.102), 6.3 (3), 6.3 (1), 6.3, 6.2.3 (110), 6.2.3, 6.2.2 .111, 6.2.2, 6.2., 6.2 (3.100), 6.2 (3), 6.2 (2), 6.2 (1), 6.2, 6.1.5 (104), 6.1.5, 6.1.4, 6.1.3, 6.1 (1-5), 6.1, 6.0.4, 6.0.3, 6.0 (4.101), 6.0 (4), 6.0 (2), 6.0 (1), 6.0, 5.3 (3), 5.3 (2), 5.3 (1.200), 5.3 (1), 5.3, 5.2 (9), 5.2 (7), 5.2 (6), 5.2 (5), 5.2 (3.210), 5.2 (2), 5.2 (1), 5.2, 5.1.4, 5.1 (4.206), 5.1, 5.0, 4.4 (8), 4.4 (7.202), 4.4 (4), 4.4, 4.3, 4.2.2, 4.2.1, 4.2 (5), 4.2, 4.1.6 b, 4.1.6, 4.0, 3.1, 3.0, 2.7	A remote Denial of Service vulnerability has been reported when handling TCP SYN packets with invalid checksums. No workaround or patch available at time of publishing. There is no exploit code required; however, an exploit has been published.	Cisco PIX Invalid TCP Checksum Remote Denial of Service CVE-2005-3774	Low	Arhont Ltd.- Information Security Advisory, November 22, 2005 **US-CERT VU#853540**
Cisco Systems Firewall Services Module (FWSM) 1.x, 2.x, IOS 12.x, IOS R12.x, PIX 4.x, 5.x, 6.x, 7.x, Cisco SAN-OS 1.x (MDS 9000 Switches), 2.x (MDS 9000 Switches), VPN 3000 Concentrator	A remote Denial of Service vulnerability has been reported due to errors in the processing of IKEv1 Phase 1 protocol exchange messages. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec.shtml **Rev 1.5: Updated Cisco IOS Products table.** Vulnerability can be reproduced with the PROTOS IPSec Test Suite.	Cisco IPSec IKE Traffic Remote Denial of Service CVE-2005-3669	Low	Cisco Security Advisory, Document ID: 68158, November 14, 2005 **Cisco Security Advisory, Document ID: 68158, Rev 1.5, November 29, 2005**
Cisco Systems IOS 12.0 (2a)	An HTTP injection vulnerability has been reported in the '/level/14/exec/buffers/assigned/ and /level/14/exec/buffers/all' scripts, 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.	Cisco IOS HTTP Service HTML Injection CVE-2005-3921	Medium	Security Focus, Bugtraq ID: 15602, November 28, 2005
Clavister Clavister Firewall 8.30.01, Security Gateway 8.40.05, 8.50.02, 8.60.01	A vulnerability has been reported in Clavister Firewall and Security Gateway that could let remote malicious users cause a Denial of Service. Vendor solution available: http://www.clavister.com/support/support_update_ISAKMP.html Currently we are not aware of any exploits for this vulnerability.	Clavister Firewall and Security Gateway Denial of Service CVE-2005-3915	Low	Secunia, Advisory: SA17663, November 24, 2005

Comdev Software Vote Caster prior to 3.1	A vulnerability has been reported in Vote Caster that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Comdev Vote Caster SQL Injection CVE-2005-3825	Medium	Security Focus, ID: 15563, November 24, 2005
Commodity Rentals CommodityRentals 2.0	An SQL injection vulnerability has been reported due to insufficient sanitization of the 'user_id' parameter in various scripts before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Commodity Rentals SQL Injection CVE-2005-3917	Medium	Secunia Advisory: SA17665, November 23, 2005
Creative Digital Resources SocketKB 1.1 .0	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'node' and 'art_id' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in the '_f' parameter due to insufficient verification before used to include files, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	SocketKB SQL Injection & File Include CVE-2005-3935 CVE-2005-3936	Medium	Secunia Advisory: SA17807, November 30, 2005
DMANews DMANews 0.904, 0.91	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'id,' 'sortorder,' and 'display_num' parameters 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. Proof of Concept exploits have been published.	DMANews SQL Injection CVE-2005-3956	Medium	Secunia Advisory: SA17759, November 29, 2005
Dotclear Dotclear 1.2.1	A vulnerability has been reported due to an unspecified error with trackbacks. Upgrade available at: http://www.dotclear.net/download/dotclear-1.2.2.tar.gz Currently we are not aware of any exploits for this vulnerability.	DotClear Unspecified Trackback CVE-2005-3957	Not Specified	Secunia Advisory: SA17769, November 9, 2005
Easybe 1-2-3 Music Store 1.0	An SQL injection vulnerability has been reported in 'process.php' due to insufficient sanitization of the 'AlbumID' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	1-2-3 Music Store SQL Injection CVE-2005-3855	Medium	Security Focus, Bugtraq ID: 15544, November 23, 2005
edmoBBS edmoBBS 0.9	An SQL injection vulnerability has been reported in the 'table' and 'messageID' parameters 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. Proof of Concept exploits have been published.	edmoBBS SQL Injection CVE-2005-3870	Medium	Security Focus, Bugtraq ID: 15589, November 28, 2005

efiction Project efiction 2.0, 1.1, 1.0	Multiple vulnerabilities have been reported: a vulnerability was reported in 'titles.php' due to insufficient sanitization of the 'let' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in the 'Manage Images' functionality due to an input validation error, which could let a remote malicious user upload valid images with an arbitrary file extension inside the web root; and a vulnerability was reported in 'phpinfo.php' because a remote malicious user can obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits and an exploit script have been published.	eFiction Input Validation	Medium	Secunia Advisory: SA17777, November 28, 2005
Entergal MX Entergal MX 2.0	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'idcat' and 'action' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Entergal MX Multiple SQL Injection CVE-2005-3958	Medium	Security Focus, Bugtraq ID: 15631, November 29, 2005
Enterprise Heart Enterprise Connector 1.0.2	An SQL injection vulnerability has been reported in 'messages.php' and 'send.php' due to insufficient sanitization of the 'meddageid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Enterprise Connector SQL Injection CVE-2005-3875	Medium	Secunia Advisory: SA17743, November 28, 2005
Fantastic Scripts Fantastic News 2.1.1	An SQL injection vulnerability has been reported in 'news.php' due to insufficient sanitization of the 'category' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Fantastic Scripts Fantastic News SQL Injection CVE-2005-3846	Medium	Secunia Advisory: SA17758, November 29, 2005
FAQ System FAQ System 1.1	SQL injection vulnerabilities have been reported in 'viewFAQ.php' due to insufficient sanitization of the 'FAQ_ID' parameter and in 'index.php' due to insufficient sanitization of the 'CATEGORY_ID' parameter, 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.	FAQ System SQL Injection CVE-2005-3943	Medium	Secunia Advisory: SA17801, November 29, 2005
freeForum 1.0, 1.0.1, 1.1	A vulnerability has been reported in freeForum that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	freeForum SQL Injection CVE-2005-3816	Medium	Security Focus, ID: 15559, November 24, 2005
FreeWebStat FreeWebStat 1.0 rev37	Cross-SIte Scripting vulnerabilities have been reported 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, Proof of Concept exploits have been published.	FreeWebStat Multiple Cross-Site Scripting CVE-2005-3959	Medium	Security Focus, Bugtraq ID: 15601, November 28, 2005

GhostScripter Amazon Shop 5.0	A Cross-Site Scripting vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'query' parameter before returning to the user, 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.	GhostScripter Amazon Shop Cross-Site Scripting CVE-2005-3908	Medium	Security Focus, Bugtraq ID: 15634, November 29, 2005
GuppY GuppY 4.5.9, 4.5.4, 4.5.3 a, 4.5.3, 4.5	Several vulnerabilities have been reported: a vulnerability was reported in 'error.php' due to insufficient sanitization of the '_SERVER[REMOTE_ADDR]' parameter before stored in a PHP script, which could let a remote malicious user execute arbitrary PHP code; and a vulnerability was reported in 'editorTypetool.php' due to insufficient verification of the 'meskin' parameter and in 'archbatch.php' and 'nwlmail.php' due to insufficient verification of the 'lng' parameter before used to include files, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits and an exploit script have been published.	GuppY Remote File Include & Command Execution CVE-2005-3926 CVE-2005-3927	High	Secunia Advisory: SA17790, November 29, 2005
Helpdesk Issue Manager Helpdesk Issue Manager 0.1-0.9	SQL injection vulnerabilities have been reported in 'find.php' due to insufficient sanitization of the 'detail[],' 'orderdir,' and 'orderby' parameters and in 'issue.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Helpdesk Issue Manager SQL Injection CVE-2005-3925	Medium	Security Focus, Bugtraq ID: 15604, November 28, 2005
Horde Project Horde 2.2-2.2.8	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of unspecified parameters before returning to the user in error messages, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/horde/horde-2.2.9.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200511-20.xml** There is no exploit code required.	Horde Error Message Cross-Site Scripting CVE-2005-3570	Medium	Secunia Advisory: SA17468, November 14, 2005 **Gentoo Linux Security Advisory, GLSA 200511-20, November 22, 2005**
Horde Project Horde prior to 3.0.7	Several vulnerabilities have been reported in the 'gzip/tar' and 'css' MIME viewers due to input validation errors, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/horde/horde-3.0.7.tar.gz Debian: http://security.debian.org/pool/updates/main/h/horde3/ There is no exploit code required.	Horde MIME Viewers Script Insertion CVE-2005-3759	Medium	Secunia Advisory: SA17703, November 23, 2005 Debian Security Advisory DSA 909-1, November 23, 2005
IPUpdate IPUpdate 1.0-1.0.3	A buffer overflow vulnerability has been reported in the 'memmcat()' function due to a boundary error when appending input, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=146709 Currently we are not aware of any exploits for this vulnerability.	IPUpdate Remote Buffer Overflow CVE-2005-3780	High	Secunia Advisory: SA17681, November 22, 2005

IsolSoft Support Center IsolSoft Support Center 2.2	An SQL injection vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'field' and 'lorder' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	IsolSoft Support Center SQL Injection CVE-2005-3838	Medium	Security Tracker Alert ID: 1015270, November 24, 2005
Kadu Kadu 0.5 pre, 0.4.2	A remote Denial of Service vulnerability has been reported when handling a specially crafted message from a Gadu-Gadu server. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Kadu Remote Denial of Service CVE-2005-3960	Low	Security Focus, Bugtraq ID: 15620, November 29, 2005
kPlaylist kPlaylist 1.6 Build 411, Build 400	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'searchfor' parameter when performing a search, 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.	kPlaylist Search Cross-Site Scripting CVE-2005-3841	Medium	Security Focus, Bugtraq ID: 15546, November 23, 2005
ltwCalendar ltwCalendar 4.1.3	An SQL injection vulnerability has been reported in 'calendar.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ltwCalendar SQL Injection	Medium	Secunia Advisory: SA17799, November 29, 2005
Macromedia Flash 7.0.19 .0, 7.0 r19, 6.0.79 .0, 6.0.65 .0, 6.0.47 .0, 6.0.40 .0, 6.0.29 .0, 6.0	A vulnerability has been reported due to insufficient validation of the frame type identifier that is read from a SWF file, which could let a remote malicious user execute arbitrary code. Update information available at: http://www.macromedia.com/devnet/security/security_zone/mpsb05-07.html Microsoft: http://www.microsoft.com/technet/security/advisory/910550.mspx SUSE: ftp://ftp.SUSE.com/pub/SUSE **Gentoo: http://security.gentoo.org/glsa/glsa-200511-21.xml** An exploit has been published.	Macromedia Flash Array Index Remote Arbitrary Code Execution CVE-2005-2628	High	Macromedia Security Advisory, MPSB05-07, November 5, 2005 Microsoft Security Advisory (910550), November 10, 2005 US-CERT VU#146284 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 **Gentoo Linux Security Advisory, GLSA 200511-21, November 25, 2005**
Mambo Mambo Site Server 4.0.14, 4.0.12 RC1-RC3, BETA & BETA 2, 4.0.10-4.0.12, 4.0	A remote file include vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary remote PHP code. **The vendor has released a patch addressing this issue. Users are advised to contact the vendor for more information on obtaining the appropriate patch.** An exploit script has been published.	Mambo Open Source Remote File Include CVE-2005-3738	High	Security Focus, Bugtraq ID: 15461, November 16, 2005 Security Focus, Bugtraq ID: 15461, November 21, 2005 **Security Focus, Bugtraq ID: 15461, November 24, 2005**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64; Inkscape 0.42, 0.41	A buffer overflow vulnerability has been reported in the SVG importer due to a boundary error, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/inkscape/ **Gentoo: http://security.gentoo.org/glsa/glsa-**	Inkscape SVG Image Buffer Overflow CVE-2005-3737	High	Ubuntu Security Notice, USN-217-1, November 21, 2005 **Gentoo Linux Security Advisory, GLSA 200511-22, November 28, 2005**

	200511-22.xml A Proof of Concept Denial of Service exploit has been published.			
Multiple Vendors University of Kansas Lynx 2.8.5 & prior	A vulnerability has been reported in the 'lynxcgi:' URI handler, which could let a remote malicious user execute arbitrary commands. Upgrades available at: http://lynx.isc.org/current/lynx2.8.6dev.15.tar.gz RedHat: http://rhn.redhat.com/errata/RHSA-2005-839.html Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200511-09.xml Trustix: http://http.trustix.org/pub/trustix/updates/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** There is no exploit code required.	Lynx URI Handlers Arbitrary Command Execution CVE-2005-2929	High	Security Tracker Alert ID: 1015195, November 11, 2005 RedHat Security Advisory, RHSA-2005:839-3, November 11, 2005 Mandriva Linux Security Advisory, MDKSA-2005:211, November 12, 2005 Gentoo Linux Security Advisory, GLSA 200511-09, November 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0066, November 22, 2005 **SGI Security Advisory, 20051101-01-U, November 29, 2005**
Multiple Vendors phpSysInfo 2.0-2.3	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user conduct Cross-Site Scripting attacks, phishing style attacks, and retrieve privileged or sensitive information. Upgrades available at: http://prdownloads.sourceforge.net/phpsysinfo/phpSysInfo-2.4.tar.gz?download Debian: http://security.debian.org/pool/updates/main/p/phpsysinfo/ Debian: http://security.debian.org/pool/updates/main/p/phpgroupware/ http://security.debian.org/pool/updates/main/e/egroupware/ Mandriva: http://wwwnew.mandriva.com/security/advisories?dis=10.2 **Gentoo:** **http://security.gentoo.org/glsa/glsa-200511-18.xml** There is no exploit code required; however, Proof of Concept exploits have been published.	phpSysInfo Multiple Vulnerabilities CVE-2005-3347 CVE-2005-3348 CVE-2003-0536	Medium	Hardened PHP Project Security Advisory, November 13, 2005 Debian Security Advisory, DSA 897-1, November 15, 2005 Debian Securities, Advisory DSA 898-1 & 899-1, November 17, 2005 Mandriva Linux Security Advisory, MDKSA-2005:212, November 16, 2005 **Gentoo Linux Security Advisory, GLSA 200511-18, November 22, 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,	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 and PEAR XML_RPC Remote Arbitrary Code Execution CVE-2005-2498	High	Security Focus, Bugtraq ID 14560, August 15, 2995 Security Focus, Bugtraq ID 14560, August 18, 2995 RedHat Security

1.0.1, 1.0.0.007, 1.0	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/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		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, 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 Debian Security Advisory, DSA 840-1, October 4, 2005 Debian Security Advisory, DSA 842-1, October 4, 2005 Conectiva Linux Announcement, CLSA-2005:1024, October 7, 2005 Security Focus, Bugtraq ID: 14560, November 7, 2005 **Fedora Legacy**

	Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/p/phpgroupware/ 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 Debian: http://security.debian.org/pool/updates/main/d/drupal/ Debian: http://security.debian.org/pool/updates/main/e/egroupware/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ b2evolution: http://prdownloads.sourceforge.net/evocms/b2evolution-0.9.1b-2005-09-16.zip?download **FedoraLegacy:** **http://download.fedoralegacy.org/** There is no exploit code required.		**Update Advisory, FLSA:166943, November 28, 2005**

Multiple Vendors RedHat Fedora Core4, Core3; PHP 5.0.4, 4.3.9	A remote Denial of Service vulnerability has been reported when parsing EXIF image data contained in corrupt JPEG files. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-831.html Mandriva: http://wwwnew.mandriva.com/security/advisories?dis=10.2 **FedoraLegacy:** **http://download.fedoralegacy.org/** **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for this vulnerability.	PHP Group Exif Module Remote Denial of Service CVE-2005-3353	Low	Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005 RedHat Security Advisory, RHSA-2005:831-15, November 10, 2005 Mandriva Linux Security Advisory, MDKSA-2005:213, November 16, 2005 **Fedora Legacy Update Advisory, FLSA:166943, November 28, 2005** **SGI Security Advisory, 20051101-01-U, November 29, 2005**
Multiple Vendors RedHat Fedora Core4, Core3; Ethereal Group Ethereal 0.10 -0.10.12, 0.9-0.9.16, 0.8.19, 0.8.18	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the ISAKMP, FC-FCS, RSVP, and ISIS LSP dissectors; a remote Denial of Service vulnerability was reported in the IrDA dissector; a buffer overflow vulnerability was reported in the SLIMP3, AgentX, and SRVLOC dissectors, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in the BER dissector; a remote Denial of Service vulnerability was reported in the SigComp UDVM dissector; a remote Denial of service vulnerability was reported due to a null pointer dereference in the SCSI, sFlow, and RTnet dissectors; a vulnerability was reported because a remote malicious user can trigger a divide by zero error in the X11 dissector; a vulnerability was reported because a remote malicious user can cause an invalid pointer to be freed in the WSP dissector; a remote Denial of Service vulnerability was reported if the 'Dissect unknown RPC program numbers' option is enabled (not the default setting); and a remote Denial of Service vulnerability was reported if SMB transaction payload reassembly is enabled (not the default setting). Upgrades available at: http://prdownloads.sourceforge.net/ethereal/ethereal-0.10.13.tar.gz?download Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-809.html Mandriva: http://www.mandriva.com/security/advisories Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-227.pdf Gentoo: http://security.gentoo.org/glsa/glsa-200510-25.xml	Ethereal Multiple Protocol Dissector Vulnerabilities CVE-2005-3184 CVE-2005-3241 CVE-2005-3242 CVE-2005-3243 CVE-2005-3244 CVE-2005-3245 CVE-2005-3246 CVE-2005-3247 CVE-2005-3248 CVE-2005-3249	High	Ethereal Security Advisory, enpa-sa-00021, October 19, 2005 Fedora Update Notifications, FEDORA-2005-1008 & 1011, October 20, 2005 RedHat Security Advisory, RHSA-2005:809-6, October 25, 2005 Mandriva Linux Security Advisory, MDKSA-2005:193, October 25, 2005 Avaya Security Advisory, ASA-2005-227, October 28, 2005 Gentoo Linux Security Advisory, GLSA 200510-25, October 30, 2005 Mandriva Linux Security Advisory, MDKSA-2005:193-2, October 31, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 **SGI Security Advisory, 20051101-01-U, November 29, 2005**

SUSE:
ftp://ftp.suse.com
/pub/suse/

SGI:
ftp://patches.sgi.com/
support/free/security/
advisories/

An exploit script has been published.

Multiple Vendors
Xoops 2.0.10-2.0.12, 2.0.9 .3, 2.0.9.2, 2.0.5-2.0.5.2, 2.0- 2.0.3; XML-RPC for PHP XML-RPC for PHP 1.1, 1.0.99 .2, 1.0.99, 1.0-1.02; WordPress 1.5-1.5.1 .2, 1.2-1.2.2, 0.71,0.7;
S9Y Serendipity 0.8.1, 0.8 -beta6 Snapshot, 0.8 -beta5 & beta6, 0.8;
PostNuke Development Team PostNuke 0.76 RC4a&b, RC4, 0.75; phpMyFAQ 1.5 RC1-RC4, 1.5 beta1-beta3, 1.5 alpha1&2, 1.4-1.4.8, 1.4;
PEAR XML_RPC 1.3 RC1-RC3, 1.3;
MandrakeSoft Linux Mandrake 10.2 x86_64, 10.2, 10.1 x86_64, 10.1, 10.0 amd64, 10.0, Corporate Server 3.0 x86_64, 3.0;
Drupal 4.6.1, 4.6, 4.5- 4.5.3
	A vulnerability was reported due to insufficient sanitization of the 'eval()' call, which could let a remote malicious user execute arbitrary PHP code.
	Drupal:
	http://drupal.org/files/projects/drupal-4.5.4.tar.gz
	Mandriva:
	http://www.mandriva.com/security/advisories
	Pear:
	http://pear.php.net/get/XML_RPC-1.3.1.tgz
	PhpMyFaq:
	http://freshmeat.net/redir/phpmyfaq/38789/url_zip/download.php
	S9Y Serendipity:
	http://prdownloads.sourceforge.net/php-blog/serendipity-0.8.2.tar.gz?download
	Trustix:
	http://http.trustix.org/pub/trustix/updates/
	WordPress:
	http://wordpress.org/latest.zip
	XML-RPC:
	http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc-1.1.1.tgz?download
	Xoops:
	http://www.xoops.org/modules/core/visit.php?cid=3&lid=62
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200507-01.xml
	http://security.gentoo.org/glsa/glsa-200507-06.xml
	http://security.gentoo.org/glsa/glsa-200507-07.xml
	http://security.gentoo.org/glsa/glsa-200507-15.xml
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/p/php4/
	Debian:
	http://security.debian.org/pool/updates/main/d/drupal/
	http://security.debian.org/pool/updates/main/p/phpgroupware/
		Multiple Vendors XML-RPC for PHP Remote Code Injection
		CVE-2005-1921
			High	Security Focus, 14088, June 29, 2005
				Gentoo Linux Security Advisory, GLSA 200507-01, July 3, 2005
				Fedora Update Notifications, FEDORA-2005-517 & 518, July 5, 2006
				Ubuntu Security Notice, USN-147-1 & USN-147-2, July 05 & 06, 2005
				US-CERT VU#442845
				Gentoo Linux Security Advisory, GLSA 200507-06, July 6, 2005
				Gentoo Linux Security Advisory, GLSA 200507-07, July 10, 2005
				SuSE Security Announcement, SUSE-SA:2005:041, July 8, 2005
				Debian Security Advisories, DSA 745-1, 747-1, & DSA 746-1, July 10 & 13, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005
				SGI Security Advisory, 20050703-01-U, July 15, 2005
				Gentoo Linux Security Advisory, GLSA 200507-15, July 15, 2005
				Debian Security Advisory, DSA 789-1, August 29, 2005
				SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005
				Security Focus, Bugtraq ID: 14088, November 7, 2005
				Security Focus, Bugtraq ID: 14088, November 23, 2005

	http://security.debian.org/pool/updates/main/e/egroupware/ SGI: http://www.sgi.com/support/security/ SuSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/ Debian: http://security.debian.org/pool/updates/main/p/php4/ SUSE: ftp://ftp.suse.com/pub/suse/ MAXdev MD-Pro Content Management: http://www.maxdev.com/Downloads-index-req-viewdownload-cid-3.phtml b2evolution: http://prdownloads.sourceforge.net/evocms/b2evolution-0.9.1b-2005-09-16.zip?download **FreeMed Software:** **http://prdownloads.sourceforge.net/freemed/freemed-0.8.1.1.tar.gz?download** Exploit scripts have been published.			
N-13 News N-13 News 1.2	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	N-13 News SQL Injection CVE-2005-3930	Medium	Secunia Advisory: SA17785, November 30, 2005
Nelogic Technologies Nephp Publisher 4.5.2	An SQL injection vulnerability has been reported in 'index.html' due to insufficient sanitization of the 'id' and 'nnet_catid' parameters 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. Proof of Concept exploits have been published.	Nelogic Nephp Publisher SQL Injection	Medium	Secunia Advisory: SA17772, November 29, 2005
Nicecoder iDesk 1.0	An SQL injection vulnerability has been reported in 'faq.php' due to insufficient sanitization of the 'cat_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Nicecoder iDesk SQL Injection CVE-2005-3843	Medium	Security Focus, Bugtraq ID: 15597, November 28, 2005
Novell ZENworks 6.5 Desktop Management, ZENworks for Desktops 4.0.1, ZENworks for Servers 3.0.2	A vulnerability has been reported in ZENworks that could let local malicious users bypass security restrictions. Vendor solution available: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2972567.htm There is no exploit code required.	Novell ZENworks Security Bypassing CVE-2005-3786	Medium	Novell, Technical Information Document TID2972567, November 23, 2005

Oliver May Athena PHP Website Administration 0.1 a	A vulnerability has been reported in 'athena.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary remote PHP 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.	Athena PHP Website Administration Remote File Include CVE-2005-3860	High	Security Focus, Bugtraq ID: 15574, November 26, 2005
Opera Software Opera Web Browser 8.50	A remote Denial of Service vulnerability has been reported when handling a Java applet containing a JNI routine. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Opera Web Browser JNI Routine Handling Remote Denia CVE-2005-3946	Low	Security Focus, Bugtraq ID: 15648, November 30, 2005
OrbitScripts Company SmartPPC Pro	A Cross-Site Scripting vulnerability has been reported in 'directory.php,' 'frames.php,' and 'search.php' due to insufficient sanitization of the 'username' parameter before returning to the user, 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.	SmartPPC Pro Cross-Site Scripting CVE-2005-3814	Medium	Security Tracker Alert ID: 1015259, November 24, 2005
Orca Blog Orca Blog 1.3 b	An SQL injection vulnerability has been reported due to insufficient sanitization of the 'msg' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Patch available at: http://www.greywyvern.com/orca#blog There is no exploit code required; however, a Proof of Concept exploit has been published.	Orca Blog SQL Injection CVE-2005-3941	Medium	Security Focus, Bugtraq ID: 15638, November 29, 2005
Orca Forum	A vulnerability has been reported in Orca Forum that could let remote malicious users perform SQL injection. Patch available at: http://www.greywyvern.com/orca#foru There is no exploit code required; however, Proof of Concept exploits have been published.	Orca Forum SQL Injection CVE-2005-3815	Medium	Security Focus, ID: 15565, November 24, 2005
Orca Knowledgebase Orca Knowledgebase2.1 b	An SQL injection vulnerability has been reported in 'knowledgebase.php' due to insufficient sanitization of the 'qid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Patch available at: http://www.greywyvern.com/orca#know There is no exploit code required; however, a Proof of Concept exploit has been published.	Orca Knowledgebase SQL Injection CVE-2005-3942	Medium	Security Focus, Bugtraq ID: 15637, November 29, 2005
Orca Ringmaker Orca Ringmaker 2.3 c	An SQL injection vulnerability has been reported in 'ringmaker.php' due to insufficient sanitization of the 'start' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Patch available at: http://www.greywyvern.com/orca#ring There is no exploit code required; however, a Proof of Concept exploit has been published.	Orca Ringmaker SQL Injection CVE-2005-3940	Medium	Security Focus, Bugtraq ID: 15639, November 30, 2005
OTRS OTRS (Open Ticket Request System) 2.0.0-2.0.3, 1.3.2, 1.0 .0	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'login' function due to insufficient sanitization of the 'login' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; an SQL injection vulnerability was reported in the 'AgentTicketPlain' function due to insufficient sanitization of the 'TicketID' and 'ArticleID' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of HTML email attachments before displaying, which could let a remote malicious user execute arbitrary HTML	OTRS SQL Injection & Cross-Site Scripting CVE-2005-3893 CVE-2005-3894 CVE-2005-3895	Medium	OTRS Security Advisory, OSA-2005-01, November 22, 2005

	and script code; and a Cross-Site Scripting vulnerability was reported in 'index.pl' due to insufficient sanitization of the 'QueueID' and 'Action' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.otrs.org/pub/otrs/otrs-1.3.3-01.tar.gz There is no exploit code required; however, Proof of Concept exploits have been published.			
OvBB Project OvBB 0.1a-0.8 a	SQL injection vulnerabilities have been reported in 'thread.php' due to insufficient sanitization of the 'threadid' parameter and in 'profile.php' due to insufficient sanitization of the 'userid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. *Note: Disputed by the vendor.* No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	OvBB Multiple SQL Injection CVE-2005-3918	Medium	Security Focus, Bugtraq ID: 15566, November 24, 2005
PBLang Team PBLang 4.65	Multiple HTML injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML 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.	PBLang Bulletin Board System Multiple HTML Injection CVE-2005-3919	Medium	Security Focus, Bugtraq ID: 15573, November 26, 2005
Pdjk-support Pdjk-support Suite 1.1 a (retail)	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'news_id,' 'faq_id,' and 'rowstart' parameters 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, Proof of Concept exploits have been published.	PDJK-support Suite Multiple SQL Injection CVE-2005-3842	Medium	Secunia Advisory: SA17722, November 25, 2005
PHP Doc System PHP Doc System 1.5.1	A vulnerability has been reported in 'index.php' due to insufficient verification of the 'show' parameter before used to include files, which could let a remote. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP Doc System Local File Include CVE-2005-3878	Medium	Secunia Advisory: SA17745, November 28, 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. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Trustix: http://http.trustix.org/pub/trustix/updates/ Upgrades available at: http://www.php.net/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-08.xml Mandriva: http://wwwnew.mandriva.com/security/advisories?dis=10.2 Trustix: http://http.trustix.org/pub/trustix/updates/ **Upgrades available at:** **http://www.php.net/get/php-4.4.1.tar.gz** There is no exploit code required.	PHP 'Open_BaseDir' Information Disclosure CVE-2005-3054	Medium	Security Focus, Bugtraq ID: 14957, September 27, 2005 Ubuntu Security Notice, USN-207-1, October 17, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 Security Focus, Bugtraq ID: 14957, October 31, 2005 Gentoo Linux Security Advisory, GLSA 200511-08, November 13, 2005 Mandriva Linux Security Advisory, MDKSA-2005:213, November 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0062, November 22, 2005 **Security Focus, Bugtraq ID: 14957, November 25, 2005**
PHP PHP 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x, 5.0.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of the 'GLOBALS' array, which could let a remote malicious user define global variables; a vulnerability was reported in the 'parse_str()' PHP function when handling an unexpected termination, which could let a remote malicious user enable the 'register_globals' directive; a Cross-Site Scripting vulnerability was reported in the 'phpinfo()' PHP function due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an integer overflow vulnerability was reported in 'pcrelib' due to an error, which could let a remote malicious user corrupt memory. Upgrades available at: http://www.php.net/get/php-4.4.1.tar.gz SUSE: ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-838.html http://rhn.redhat.com/errata/RHSA-2005-831.html Gentoo: http://security.gentoo.org/glsa/glsa-200511-08.xml Mandriva: http://wwwnew.mandriva.com/security/advisories?dis=10.2	PHP Multiple Vulnerabilities CVE-2005-3388 CVE-2005-3389 CVE-2005-3390 CVE-2005-3391 CVE-2005-3392	Medium	Secunia Advisory: SA17371, October 31, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Turbolinux Security Advisory TLSA-2005-97, November 5, 2005 Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005 RedHat Security Advisories, RHSA-2005:838-3 & RHSA-2005:831-15, November 10, 2005 Gentoo Linux Security Advisory, GLSA 200511-08, November 13, 2005 Mandriva Linux Security Advisory, MDKSA-2005:213, November 16, 2005 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0062, November 22, 2005 **SGI Security Advisory, 20051101-01-U, November 29, 2005**

	SUSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** There is no exploit code required.			
PHP Upload Center PHP Upload Center	A Directory Traversal vulnerability has been reported which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP Upload Center Directory Traversal CVE-2005-3947	Medium	Security Focus, Bugtraq ID: 15626, November 29, 2005
phpAlbum.net phpalbum 0.2.3	A file include vulnerability was reported which could let a remote malicious user execute arbitrary server-side 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.	PHPAlbum File Include CVE-2005-3948	Medium	Security Focus, Bugtraq ID: 15651, November 30, 2005
phpGreetz phpGreetz 0.99	A vulnerability has been reported in 'content.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPGreetz Remote File Include CVE-2005-3861	High	Security Focus, Bugtraq ID: 15575, November 26, 2005
PHP PHP 5.0 .0- 5.0.5, 4.4.1, 4.4 .0, 4.3-4.3.11, 4.2-4.2.3, 4.1.0-4.1.2, 4.0.6, 4.0.7, RC1-RC3	A vulnerability has been reported in the 'mb_send_mail()' function due to an input validation error, which could let a remote malicious user inject arbitrary headers to generated email messages. Upgrades available at: http://www.php.net/get/php-5.1.0.tar.bz2/from/a/mirror There is no exploit code required.	PHP MB_Send_Mail Arbitrary Header Injection CVE-2005-3883	Medium	Security Focus, Bugtraq ID: 15571, November 25, 2005
PHPPost PHPPost 1.0	An HTML injection 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. No workaround or patch available at time of publishing. There is no exploit code required.	PHPPost Subject HTML Injection CVE-2005-3770	Medium	Security Focus, Bugtraq ID: 15532, November 22, 2005
PHPWeb Statistik PHPWebStatistik 1.4	Multiple vulnerabilities have been reported: a vulnerability was reported in 'stat.php' due to insufficient sanitization of the 'lastnumber' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported due to the insecure storage of configuration and database files inside the web root, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in 'stat.php' due to insufficient verification of the 'lastnumber' parameter before using in an loop statement, which could let a remote malicious user cause a Denial of Service; and a vulnerability was reported due to insufficient sanitization of the 'referer' header, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	PHP Web Statistik Multiple Vulnerabilities	Medium	Secunia Advisory: SA17789, November 29, 2005

PmWiki PmWiki 2.0.0-2.0.12	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'q' parameter when performing a search, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.pmwiki.org/pub/pmwiki/pmwiki-2.0.13.tgz There is no exploit code required; however, a Proof of Concept exploit has been published.	PmWiki Cross-Site Scripting CVE-2005-3849	Medium	Security Focus, Bugtraq ID: 15539, November 23, 2005
Q-News Q-News 2.0	A vulnerability has been reported in 'q-news.php' due to insufficient verification of the 'id' parameter before used to include files, which could let a remote malicious user execute arbitrary remote PHP 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.	Q-News Remote File Include CVE-2005-3859	High	Security Focus, Bugtraq ID: 15576, November 27, 2005
QNX Software Systems Ltd. RTOS 6.3 .0	A buffer overflow vulnerability has been in 'Phgrafx' because the affected utility has setuid-superuser privileges, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	QNX Phgrafx Buffer Overflow CVE-2005-3928	High	Security Focus, Bugtraq ID: 15619, November 29, 2005
Quality Unit Post Affiliate Pro 2.0.4	Several vulnerabilities have been reported: an SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'sortorder' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a file include vulnerability was reported in 'merchants/index.php,' which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Post Affiliate Pro SQL Injection & File Include CVE-2005-3909 CVE-2005-3910	Medium	Secunia Advisory: SA17751, November 29, 2005
randgruppe Randshop	SQL injection vulnerabilities have been reported in 'themes/kategorie/index.php' due to insufficient sanitization of the 'kategorieied' and 'katid' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Randshop SQL Injection CVE-2005-3924	Medium	Security Focus, Bugtraq ID: 15599, November 28, 2005
Real Soft Studio UGroup 2.6.2	SQL injection vulnerabilities have been reported in 'forum.php' due to insufficient sanitization of the 'FORUM_ID' parameter and in 'topic.php' due to insufficient sanitization of the 'TOPIC_ID' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Proof of Concept exploits have been published.	UGroup SQL Injection CVE-2005-3872	Medium	Secunia Advisory: SA17734, November 28, 2005
Scripts-Templates AllWeb Search 3.0	An SQL injection vulnerability has been reported in the 'search' parameter before using in an SQL query. which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	AllWeb Search SQL Injection CVE-2005-3865	Medium	Security Focus, Bugtraq ID: 15587, November 28, 2005
sCssBoard 1.0, 1.1, 1.11, 1.12, 1.2	A vulnerability has been reported in sCssBoard that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	sCssBoard Cross-Site Scripting CVE-2005-3837	Medium	Secunia, Advisory: SA17716, November 24, 2005
SearchSolutions SearchFeed Search Engine 1.3.2; RevenuePilot Search Engine 1.2.0; Google API Search Engine 1.3.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'REQ' parameter when performing a search, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing.	SearchSolutions Cross-Site Scripting CVE-2005-3866 CVE-2005-3867	Medium	Security Focus, Bugtraq ID: 15612, November 29, 2005

	There is no exploit code required; however, a Proof of Concept exploit has been published.	CVE-2005-3869		
Sensation Designs KBase Express 1.0.0	SQL injection vulnerabilities have been reported in 'category.php' due to insufficient sanitization of the 'id' parameter and certain parameters when performing a search, 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.	KBase Express Multiple SQL Injection CVE-2005-3880	Medium	Security Focus, Bugtraq ID: 15635, November 29, 2005
Sergids Top Music Module 3.0 PR3	SQL injection vulnerabilities have been reported in 'idartist,' 'idsong,' and 'idalbum' parameters due to insufficient sanitization before using in a SQL, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Top Music Module SQL Injection	Medium	Security Focus, Bugtraq ID: 15581, November 28, 2005
Simple Document Management System Simple Document Management System 2.0 -CVS	An SLQ injection vulnerability has been reported in 'message.php' due to insufficient sanitization of the 'mid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Proof of Concept exploits have been published.	Simple Document Management System SQL Injection CVE-2005-3877	Medium	Security Focus, Bugtraq ID: 15596, November 28, 2005
SimpleMedia SimpleBBS 1.1	An SQL injection vulnerability has been reported in the search module parameters due to insufficient sanitization of user-supplied input 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.	SimpleBBS SQL Injection	Medium	Security Focus, Bugtraq ID: 15594, November 28, 2005
SoftBizScripts B2B trading Marketplace Script 1.1	An SQL injection vulnerability has been reported in 'selloffers.php,' 'buyoffers.php,' 'products.php,' and 'profiles.php' due to insufficient sanitization of the 'cid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Softbiz B2B Trading Marketplace Script SQL Injection CVE-2005-3937	Medium	Secunia Advisory: SA17808, November 30, 2005
SoftbizScripts Softbiz FAQ Script 1.1 & prior	SQL injection vulnerabilities have been reported in 'faq_qanda.php,' 'refer_friend.php,' 'print_article.php,' and 'add_comment.php' due to insufficient sanitization of the 'id' parameter and in 'index.php' due to insufficient sanitization of the 'cid' parameter before being used 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, Proof of Concept exploits have been published.	Softbiz FAQ Script SQL Injection CVE-2005-3938	Medium	Secunia Advisory: SA17809, November 30, 2005
SoftbizScripts Softbiz Web Host Directory Script 1.1	A vulnerability has been reported in Softbiz Web Host Directory Script that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Softbiz Web Host Directory Script SQL Injection CVE-2005-3817	Medium	Secunia, Advisory: SA17724, November 24, 2005
SourceShock ShockBoard 4.0, 3.0	An SQL injection vulnerability has been reported in 'topic.php' due to insufficient sanitization of the 'offset' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ShockBoard SQL Injection CVE-2005-3873	Medium	Security Focus, Bugtraq ID: 15592, November 28, 2005

SpoonLabs phpWordPress 3.0	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'poll,' 'category,' and 'ctg' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	phpWordPress SQL Injection CVE-2005-3844	Medium	Secunia Advisory: SA17733, November 25, 2005
Sun Microsystems, Inc. Java JDK 1.5.x, Java JRE 1.3.x, 1.4.x, 1.5.x / 5.x, Java SDK 1.3.x, 1.4.x	Several vulnerabilities have been reported: a vulnerability was reported due to an unspecified error, which could let a malicious untrusted applet read/ write local files or execute local applications; three unspecified vulnerabilities were reported with the use of 'reflection' APIs error, which could let a malicious untrusted applet read/write local files or execute local applications; and a vulnerability was reported in the Java Management Extensions (JMX) implementation, which could let a malicious untrusted applet read/ write local files or execute local applications. Upgrade information available at: http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102003-1 http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102017-1 http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102050-1 Currently we are not aware of any exploits for these vulnerabilities.	Sun Java Runtime Environment Security Bypass CVE-2005-3904 CVE-2005-3905 CVE-2005-3906 CVE-2005-3907	Medium	Sun(sm) Alert Notifications Sun Alert ID: 102003, 102017, & 102050, November 28, 2005
SupportPRO SupportDesk 1.12	A vulnerability has been reported in SupportPRO SupportDesk that could let remote malicious users perform Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	SupportPRO SupportDesk Cross-Site Scripting CVE-2005-3839	Medium	Secunia, Advisory: SA17701, November 24, 2005
Survey System Survey System 1.1	An SQL injection vulnerability has been reported in 'survey.php' due to insufficient sanitization of the 'SURVEY_ID' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Survey System SQL Injection CVE-2005-3944	Medium	Security Focus, Bugtraq ID: 15641, November 30, 2005
Turn-K K-Search 1.0	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'id,' 'stat,' and 'source' parameters 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. Proof of Concept exploits have been published.	K-Search SQL Injection CVE-2005-3868	Medium	Secunia Advisory: SA17719, November 28, 2005
vTiger CRM 4.2 & prior	Multiple vulnerabilities have been reported in vTiger CRM that could let remote malicious users bypass security restrictions, conduct Cross-Site Scripting, disclose information, or execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	vTiger CRM Multiple Vulnerabilities CVE-2005-3818 CVE-2005-3819 CVE-2005-3820 CVE-2005-3821 CVE-2005-3822 CVE-2005-3823 CVE-2005-3824	High	Secunia, Advisory: SA17693, November 24, 2005
Weaverslave Netzbrett 1.5.1	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'p_entry' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Netzbrett SQL Injection CVE-2005-3874	Medium	Security Focus, Bugtraq ID: 15593, November 28, 2005

WebCalendar WebCalendar 1.0.1	Several vulnerabilities have been reported: SQL injection vulnerabilities were reported due to insufficient sanitization of 'export_handler.php,' 'activity_log.php,' 'admin_handler.php,' and 'edit_template.php' before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'export_handler.php' due to insufficient verification of the 'id' and 'format' parameters before used to save data files, which could let a remote malicious user overwrite saved data files. No workaround or patch available at time of publishing. There is no exploit code required.	WebCalendar SQL Injection & File Overwrite CVE-2005-3949 CVE-2005-3961	Medium	Secunia Advisory: SA17784, November 29, 2005
WSN Forum WSN Forum 1.21	An SQL injection vulnerability has been reported in 'memberlist.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WSN Forum SQL Injection CVE-2005-3916	Medium	Security Focus, Bugtraq ID: 15549, November 23, 2005
Xaraya Xaraya 1.0 RC1-RC4	A Directory Traversal vulnerability has been reported in the 'index.php' script 'module' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Xaraya Directory Traversal CVE-2005-3929	Medium	Security Focus, Bugtraq ID: 15623, November 29, 2005
Zainu Zainu 2.0	SQL injection vulnerabilities have been reported in the 'term' and 'start' parameters 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. A Proof of Concept exploit has been published.	Zainu SQL Injection CVE-2005-3884	Medium	Bugtraq ID: 15579, November 28, 2005

[back to top]

Wireless

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

- **Mobile Java gets an upgrade:** The Mobile Service Architecture initiative was set up by Vodafone and Nokia and includes major players in the mobile industry. They are grouping together to develop new standards for mobile Java. New standards are being designed to simplify the development environment and make it easier for phones to interoperate. Source: http://www.itweek.co.uk/vnunet/news/2146546/mobile-java-gets-upgrade

Wireless Vulnerabilities

- Nothing significant to report.

[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
November 30, 2005	centericq_dos.c	Yes	Proof of Concept exploit for the CenterICQ Malformed Packet Handling Remote Denial of Service vulnerability.
November 30, 2005	kapda-phpp.txt	No	Exploitation details for the PHPP Cross-Site Scripting vulnerability.
November 30, 2005	NukeETSQL32.txt	Yes	Exploit details for the Tru-Zone Nuke ET SQL Injection vulnerability.
November 30, 2005	OperaTest.java	No	Proof of Concept exploit for the Opera Web Browser JNI Routine Handling Remote Denial of Service vulnerability.
November 30, 2005	poc.tgz	Yes	Proof of Concept html for the Microsoft Internet Explorer Unauthorized Access vulnerability.
November 30, 2005	SmartPPCProXSS.txt	No	Exploit details for the SmartPPC Pro Cross-Site Scripting vulnerability.

November 30, 2005	smuggler.c	N/A	Smuggler demonstrates HTTP Request Smuggling techniques.
November 29, 2005	linux_lock_lease_dos.c	Yes	Script that exploits the Linux Kernel Time_Out_Leases PrintK Local Denial of Service vulnerability.
November 29, 2005	qnx_phgrafx_bof.c	No	Script that exploits the QNX Phgrafx Buffer Overflow vulnerability.
November 28, 2005	alzgen.pl	Yes	Perl script that exploits the Unalz Archive Filename Buffer Overflow vulnerability.
November 28, 2005	guppy_inc.php	No	Script that exploits the GuppY Remote File Include & Command Execution vulnerabilities.
November 25, 2005	efiction20_xpl.php efiction2_xpl.txt	No	Exploit for the eFiction Input Validation vulnerabilities.
November 24, 2005	freeFTPd-dos.c	No	Proof of Concept exploit for the FreeFTPD Multiple Denial of Service vulnerability.

[back to top]

Trends

- **Phishing email poses as IRS tax refund:** According to Sophos, lax government security around a US government website has allowed email fraudsters to run a scam designed to trick US taxpayers into handing over sensitive personal information. A phishing email which pose as notification of a refund from the US's Internal Revenue Service (IRS) takes advantage of security configuration weaknesses on a secondary website run by the Department of Labor. The email redirect surfers to a bogus website with users fooled into thinking they remain on a legitimate US government site. Source: http://www.theregister.com/2005/11/30/irs_phishing_scam/
- **Cybercrime yields more cash than drugs: expert:** According to a top expert, global cybercrime generated a higher turnover than drug trafficking in 2004 and is set to grow even further with the wider use of technology in developing countries. No country is immune from cybercrime, which includes corporate espionage, child pornography, stock manipulation, extortion and piracy. Source: http://today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2005-11-28T200056Z_01_KWA867007_RTRUKOC_0_US-CYBER
- **Mac OS X security under scrutiny:** When the SANS Institute released its Top-20 vulnerabilities last week, they called out an entire operating system for its vulnerabilities. This year, the list flagged the collective vulnerabilities in Apple Computer's Mac OS X operating system as a major threat. While the move has raised questions about the value of such a general warning, highlighting recent vulnerabilities in Mac OS X was intended as a wake up call, Source: http://www.securityfocus.com/news/11359
- **Vulnerability in Cisco PIX**: US-CERT is aware of a publicly reported vulnerability in the way Cisco PIX firewalls process legitimate TCP connection attempts. Source: http://www.us-cert.gov/current/.
- **Can You Spot The Phishing Attack?** According to the e-mail security firm, MailFrontier, only 4 percent of users can spot a phished e-mail 100 percent of the time. Knowing the difference between a legitimate e-mail and a scammed phishing e-mail is not always easy. This data comes from MailFrontier's Phishing IQ Test, which is comprised of 10 examples of e-mails and users must choose whether they think the mail is legitimate, a fraud or if they have no answer. Source: http://www.esecurityplanet.com/best_practices/article.php/3566651

[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	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 anti virus, and modifying data.
3	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.
4	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.

5	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.
6	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.
7	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
8	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.
9	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.
10	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.

Table updated November 25, 2005

[back to top]

Last updated December 01, 2005