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

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

Vulnerabilities

- Windows Operating Systems
  - Alt-N MDaemon and WorldClient Denial of Service
  - ASPBB Information Disclosure
  - ASP-DEV XM Forum Cross Site Scripting
  - ASPMForum SQL Injection
  - CF Nuke Cross-Site Scripting or Information Disclosure
  - LocazoList Classifieds Cross-Site Scripting
  - LogiSphere Denial of Service
  - **Microsoft DirectX DirectShow Arbitrary Code Execution (Updated)**
  - Microsoft Excel Arbitrary Code Execution
  - **Microsoft Internet Explorer Unauthorized Access (Updated)**
  - Microsoft Internet Explorer Arbitrary Code Execution
  - Microsoft Internet Explorer Arbitrary Code Execution
  - Microsoft Internet Explorer Information Disclosure
  - Microsoft Windows Privilege Elevation
  - **Microsoft Windows SMB Buffer Overflow (Updated)**
  - My Album Information Disclosure
  - Opera Web Browser Download Dialog File Manipulation
  - Sights 'n Sounds Streaming Media Server Denial of Service
  - **Sony SunnComm MediaMax Insecure Directory Permissions (Updated)**
  - Trend Micro ServerProtect Multiple Vulnerabilities
- UNIX / Linux Operating Systems
  - Apple Mac OS X Perl Privilege Dropping
  - CartKeeper CKGold Cross-Site Scripting
  - **cURL / libcURL URL Parser Buffer Overflow (Updated)**

- DRZES HMS Cross-Site Scripting & SQL Injection
- Horde Mnemo Remote HTML Injection
- Horde Turba Multiple HTML Injection
- Horde Application Framework HTML Injection
- Horde Kronolith HTML Injection
- Horde Nag Remote HTML Injection
- **IPsec-Tools ISAKMP IKE Remote Denial of Service (Updated)**
- **Mike Neuman OSH Remote Buffer Overflow (Updated)**
- **Mike Neuman OSH Command Line Argument Buffer Overflow (Updated)**
- **Mozilla Firefox Multiple Vulnerabilities (Updated)**
- **Multiple Vendors Xpdf Buffer Overflows (Updated)**
- **Multiple Vendors Linux Kernel IPV6 Denial of Service (Updated)**
- Multiple Vendors Linux Kernel Integer Overflow
- **PHPMyAdmin Multiple Cross-Site Scripting (Updated)**
- **Multiple Vendors Linux Kernel Find_Target Local Denial of Service (Updated)**
- **Multiple Vendors Linux Kernel 64 Bit PTrace Kernel Memory Access (Updated)**
- **Multiple Vendors Linux Kernel Stack Fault Exceptions Denial of Services (Updated)**
- **Multiple Vendors Linux Kernel XFRM Array Index Buffer Overflow (Updated)**
- **Multiple Vendors Linux Kernel do_coredump Denial of Service (Updated)**
- Positive Software Corporation CP+ Unspecified Perl Remote Denial of Service
- **Linux Kernel ZLib Null Pointer Dereference Denial of Service (Updated)**
- **Multiple Vendors Linux Kernel 'ptrace()' Denial of Service (Updated)**
- **Multiple Vendors Linux Kernel Network Bridge Information Disclosure (Updated)**
- **Multiple Vendors Linux Kernel 'MMap()' Denial of Service (Updated)**
- Multiple Vendors Courier Mail Server Unauthorized Access
- **Multiple Vendors Linux Kernel Race Condition and Buffer Overflow (Updated)**
- **Multiple Vendors Linux Kernel 64 Bit 'AR-RSC' Register Access (Updated)**
- **Multiple Vendors Linux Kernel SYSFS_Write_File Local Integer Overflow (Updated)**
- **Multiple Vendors Linux Kernel Radionet Open Source Environment (ROSE) ndigis Input Validation (Updated)**

- Multiple Vendors Linux Kernel 64 Bit EXT3 Filesystem Extended Attribute Denial of Service (Updated)
- Multiple Vendors Linux Kernel 'Fib_Seq_Start' Denial of Service (Updated)
- Multiple Vendors Linux Kernel File Lock Lease Local Denial of Service (Updated)
- Multiple Vendors Linux Kernel EXT2/EXT3 File Access Bypass (Updated)
- Multiple Vendors Linux Kernel 'Ipt_recent' Remote Denial of Service (Updated)
- Multiple Vendors Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service (Updated)
- Multiple Vendors Linux Kernel Denial of Service (Updated)
- Multiple Vendors Linux Kernel Remote Denial of Service (Updated)
- Multiple Vendors Linux Kernel routing_ioctl() Denial of Service (Updated)
- Multiple Vendors Linux Kernel Denial of Service & Information Disclosure (Updated)
- Multiple Vendors Linux Kernel USB Subsystem Denials of Service (Updated)
- Multiple Vendors Linux Kernel Denial of Service (Updated)
- Multiple Vendors Linux Kernel Console Keymap Arbitrary Command Injection (Updated)
- Multiple Vendors Linux Kernel PTrace 'CLONE_THREAD' Denial of Service (Updated)
- Multiple Vendors Linux Kernel PrintK Local Denial of Service (Updated)
- Multiple Vendors Linux Kernel PTraced Denial of Service (Updated
- Multiple Vendor WGet/Curl NTLM Username Buffer Overflow (Updated)
- Multiple Vendors Linux Kernel POSIX Timer Cleanup Handling Local Denial of Service (Updated)
- Multiple Vendors Linux Kernel IPv6 FlowLable Denial of Service (Updated)
- Multiple Vendors Linux Kernel SNMP Handler Remote Denial of Service (Updated)
- Multiple Vendors Linux Kernel Resource Leak Denial of Service (Updated)
- Multiple Vendors Linux Kernel ISO File System Remote Denial of Service (Updated)
- Linux Kernel ZLib Invalid Memory Access Denial of Service (Updated)
- Multiple Vendors Linux Kernel SCSI ProcFS Denial

of Service (Updated)
    - **Multiple Vendors Linux Kernel Information Disclosure (Updated)**
    - **Multiple Vendors Perl 'miniserv.pl' script Format String (Updated)**
    - MySQL Auction Cross-Site Scripting
    - **Openswan IKE Message Remote Denials of Service (Updated)**
    - **OpenVPN Client Remote Format String & Denial of Service (Updated)**
    - **PHPMyAdmin 'Import_Blacklist' Variable Overwrite (Updated)**
    - SCO UnixWare Buffer Overflow
    - Scout Portal Toolkit Cross-Site Scripting &SQL Injection
    - Sun Solaris Sun Update Connection Web Proxy Password Disclosure
    - **UW-imapd Denial of Service and Arbitrary Code Execution (Updated)**
    - **Zope 'RestructuredText' Unspecified Security Vulnerability (Updated)**
- Multiple Operating Systems
    - ACME Perl-Cal Cross-Site Scripting
    - Apache James Spooler Memory Leak Remote Denial of Service
    - Apache mod_imap Cross-Site Scripting
    - Apani Networks EpiForce IPSec IKE Processing Remote Denial of Service
    - Arab Portal SQL Injection
    - Blackboard Academic Suite Cross-Domain
    - CFMagic Multiple Products Input Validation
    - Magic Book Professional Cross-Site Scripting
    - CA CleverPath Portal Cross-Site Scripting
    - Contenido CMS Remote Command Execution
    - CourseForum Technologies ProjectForum Cross-Site Scripting & Denial of Service
    - Dell TrueMobile 2300 Remote Authentication Bypass
    - **DoceboLMS Directory Traversal & File Upload (Updated)**
    - DreamLevels Dream Poll SQL Injection
    - Envolution SQL Injection & Cross-Site Scripting
    - Ethereal OSPF Protocol Dissection Buffer Overflow
    - EveryAuction Cross-Site Scripting
    - **FFmpeg Remote Buffer Overflow (Updated)**
    - **First 4 Internet CodeSupport Remote Arbitrary Code Execution (Updated)**
    - Flatnuke Elevated Privileges & Remote Command Execution
    - PHPNuke Content Filtering Bypass
    - **HP OpenView Network Node Manager Remote Arbitrary Code Execution (Updated)**

- Jamit Job Board SQL Injection
- Guestserver HTML Injection
- Multiple Linksys Routers Remote Denial of Service
- Lyris ListManager Multiple Vulnerabilities
- Macromedia Flash Media Server Administration Service Denial of Service
- **Mambo Open Source Remote File Include (Updated)**
- Mantis Cross-Site Scripting
- mcGalleryPRO Multiple Vulnerabilities
- **MediaWiki HTML Inline Style Attributes Cross-Site Scripting (Updated)**
- Milliscripts Cross-Site Scripting
- Motorola SB5100E Cable Modem Remote Denial of Service
- Mozilla History File Remote Denial of Service
- **Multiple Vendors PHP Group Exif Module Remote Denial of Service (Updated)**
- **Multiple Vendors XML-RPC for PHP Remote Code Injection (Updated)**
- MyBB SQL Injection & Unspecified Vulnerabilities
- NetGear RP114 SYN Flood Denial of Service
- Netref SQL Injection Scripting
- Nortel SSL VPN Web Interface Input Validation
- **OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials (Updated)**
- Opera Web Browser Long Page Title Remote Denial of Service
- PGP Desktop Wipe Free Space Assistant Improper Disk Wipe
- PHP JackKnife Gallery System Cross-Site Scripting
- **PHP Multiple Vulnerabilities (Updated)**
- PHP Web Scripts Ad Manager Pro SQL Injection
- Link Up Gold Cross-Site Scripting
- PHPCoin SQL Injection
- PHPCoin File Include
- **PHP MB_Send_Mail Arbitrary Header Injection (Updated)**
- PHPWebGallery SQL Injection
- Plogger SQL Injection & Cross-Site Scripting
- EncapsGallery SQL Injection
- QNX RTOS 'dhcp.client' File Permission
- Simple Machines Forum SQL Injection
- SimpleBBS Input Validation
- Snipe Gallery Cross-Site Scripting & SQL Injection
- ThWboard Multiple Input Validation
- Triangle Solutions PHP Support Tickets Multiple SQL Injection
- UseBB Cross-Site Scripting
- VCD-db Cross-Site Scripting & Path Disclosure

  - Website Baker SQL Injection
  - WHMCompleteSolution Cross-Site Scripting
  - WikkaWiki Cross-Site Scripting
  - **XMail Command Line Buffer Overflow (Updated)**

Wireless

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

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
Alt-N MDaemon 8.1.3, WorldClient	A vulnerability has been reported in MDaemon and WorldClient that could let remote malicious users perform a Denial of Service.	Alt-N MDaemon and WorldClient Denial of Service	Low	Security Focus, ID: 15815, December 12, 2005

8.1.3	No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	CVE-2005-4265 CVE-2005-4266		
ASPBB ASPBB 0.4	Multiple vulnerabilities have been reported in ASPBB that could let remote malicious users obtain 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.	ASPBB Information Disclosure	Medium	Security Focus, ID: 15859, December 14, 2005
ASP-Dev XM Forum RC3	A vulnerability has been reported in XM Forum that could let remote malicious users conduct cross site scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ASP-DEV XM Forum Cross Site Scripting	Medium	Security Focus, ID: 15858, December 14, 2005
ASPM Forum	Multiple vulnerabilities have been reported in ASPMForum 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.	ASPMForum SQL Injection CVE-2005-4141	Medium	Secunia, Advisory: SA17954, December 8, 2005
CF_Nuke CF_Nuke 4.6	A directory traversal vulnerability has been reported in CF_Nuke that could let remote malicious users conduct Cross-Site Scripting or disclose 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.	CF_Nuke Cross-Site Scripting or Information Disclosure CVE-2005-4074 CVE-2005-4075	Medium	Security Focus, ID: 15777, 15778, December 8, 2005

LocazoList LocazoList Classifieds 1.0 3c	A vulnerability has been reported in LocazoList Classifieds that could let remote malicious users conduct Cross-Site Scripting. A vendor solution is available: http://locazo.net:81/applications/ There is no exploit code required; however, a Proof of Concept exploit has been published.	LocazoList Classifieds Cross-Site Scripting CVE-2005-4205	Medium	Security Focus, ID: 15812, December 12, 2005
LogiSphere LogiSphere 0.9.9j	A directory traversal vulnerability has been reported in LogiSphere 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.	LogiSphere Denial of Service CVE-2005-4203	Low	Secunia, Advisory: SA17989, December 12, 2005

Microsoft DirectX DirectShow 7.0 to 9.0c	A buffer overflow vulnerability has been reported in DirectX DirectShow that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-050.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=366955&RenditionID= V1.3 Updated to note availability of Microsoft Knowledge Base Article 909596 and to clarify an issue affecting Windows 2000 SP4 customers, also updates of file versions. V1.4 Updated to note complications of the DirectX 8.1 update on machines running DirectX 9. **V2.0 Updated to advise customers that a** **new version of the security update is available for select systems.** Currently we are not aware of any exploits for this vulnerability.	Microsoft DirectX DirectShow Arbitrary Code Execution CVE-2005-2128	High	Microsoft, Security Bulletin MS05-050, October 11, 2005 USCERT, VU#995220 Technical Cyber Security Alert TA05-284A, October 11, 2005 Avaya, ASA-2005-214, October 11, 2005 Microsoft, Security Bulletin MS05-050 V1.3, October 21, 2005 Microsoft, Security Bulletin MS05-050 V1.4, November 9, 2005 Nortel, Security Advisory Bulletin 2005006315, November 11, 2005 **Microsoft, Security Bulletin MS05-050 V2.0, December 13, 2005**
Microsoft Excel	A stack overflow vulnerability has been reported in Microsoft Excel that could let local or remote malicious users execute arbitrary code. No workaround or patch available at time of publishing.	Microsoft Excel Arbitrary Code Execution CVE-2005-4131	High	Security Tracker, Alert ID: 1015333, December 8, 2005

	An exploit has been published.			
Microsoft Internet Explorer	A vulnerability has been reported in Internet Explorer, by mismatched DOM objects, that could let remote malicious users to obtain unauthorized access. Vendor solutions available: http://www.microsoft.com/technet/security/advisory/911302.mspx **http://www.microsoft.com/technet/security/Bulletin/MS05-054.mspx** **An exploit has been published.**	Microsoft Internet Explorer Unauthorized Access CVE-2005-1790	Medium	Microsoft, Security Advisory 911302, November 21, 2005 USCERT, VU#887861, November 21, 2005 **Microsoft, Security Bulletin MS05-054, December 13, 2005**
Microsoft Internet Explorer 6.0 SP1 and prior	A vulnerability has been reported in Internet Explorer, by dialog manipulation, that could let remote malicious users execute arbitrary code. A vendor solution is available: http://www.microsoft.com/technet/security/Bulletin/MS05-054.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2005-2829	High	Microsoft, Security Bulletin MS05-054, December 13, 2005
Microsoft Internet Explorer 6.0 SP1 and prior	A vulnerability has been reported in Internet Explorer, COM object Instantiation, that could let remote malicious users execute arbitrary code. A vendor solution is available: http://www.microsoft.com/technet/security/Bulletin/MS05-054.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2005-2831	High	Microsoft, Security Bulletin MS05-054, December 13, 2005
Microsoft Internet Explorer 6.0 SP1 and prior	A vulnerability has been reported in Internet Explorer that could let remote malicious users disclose information. A vendor solution is available: http://www.microsoft.com/technet/security/Bulletin/MS05-054.mspx There is no exploit code required.	Microsoft Internet Explorer Information Disclosure CVE-2005-2830	Medium	Microsoft, Security Bulletin MS05-054, December 13, 2005

Microsoft Windows 2000 Server SP4 and prior, Professional SP4 and prior, Datacenter Server SP4 and prior, Advanced Server SP4 and prior	A vulnerability has been reported in Windows, Asynchronous Procedure Calls, that could let local malicious users obtain elevated privileges. A vendor solution is available: http://www.microsoft.com/technet/security/Bulletin/MS05-055.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Privilege Elevation CVE-2005-2827	Medium	Microsoft, Security Bulletin MS05-055, December 13, 2005
Microsoft Windows 2000 SP3 & SP4, Windows XP 64-Bit Edition SP1 (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	A buffer overflow vulnerability exists when handling Server Message Block (SMB) traffic, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-011.mspx Microsoft Windows NT 4.0 has also been found vulnerable to the issue; however, this platform is no longer publicly supported by Microsoft. A patch is available for customers that have an active end-of-life support agreement including extended Windows NT 4.0 support. Information regarding the end-of-life support agreement can be found at the following location: http://www.microsoft.com/presspass/features/2004/dec04/12-03NTSupport.asp **V1.1 Revised to advise of Knowledge Base Article 896427, detailing a potential issue encountered after installing this update.** An exploit has been published.	Microsoft Windows SMB Buffer Overflow CVE-2005-0045	High	Microsoft Security Bulletin, MS05-011, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#652537 Security Focus, 12484, March 9, 2005 Security Focus, Bugtraq ID: 12484, June 23, 2005 **Microsoft Security Bulletin, MS05-011 V1.1, December 13, 2005**

My Album My Album 1.0	A directory traversal vulnerability has been reported in My Album that could let remote malicious users disclose 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.	My Album Information Disclosure CVE-2005-4201	Medium	Secunia, Advisory: SA17951, December 12, 2005
Opera Software Opera Web Browser 8.0 1	A vulnerability has been reported because a remote malicious user can hide a 'File Download' dialog box underneath a new browser window and entice a user into double clicking a specific area in the window, which could lead to the remote arbitrary code execution. Update to 8.02 or later: http://www.opera.com/download/ Currently we are not aware of any exploits for this vulnerability.	Opera Web Browser Download Dialog File Manipulation CVE-2005-2407	High	Secunia Advisory: SA15781, December 13, 2005
Sights 'n Sounds Streaming Media Server 2.0.3.b	A buffer overflow vulnerability has been reported in Streaming Media Server 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.	Sights 'n Sounds Streaming Media Server Denial of Service CVE-2005-4194	Low	Secunia, Advisory: SA17998, December 12, 2005
Sony SunnComm MediaMax 5.0.21.0	A vulnerability has been reported due to insecure default directory ACLs set on the 'SunnComm Shared' directory, which could let a malicious user obtain elevated privileges. Patch available at: http://www.sunncomm.com/support/updates/updates.asp **http://www.sonybmg.com/indexmediamax.html** **Entry erroneously listed as Multiple OS.** There is no exploit code required.	Sony SunnComm MediaMax Insecure Directory Permissions CVE-2005-4069	Medium	Secunia Advisory: SA17933, December 7, 2005 **Security Tracker, Alert ID: 1015327, December 8, 2005**

Trend Micro ServerProtect 5.58	Multiple vulnerabilities have been reported in ServerProtect that could let remote malicious users cause a Denial of Service or obtain information. Contact the vendor for workaround and fix. There is no exploit code required.	Trend Micro ServerProtect Multiple Vulnerabilities CVE-2005-1928 CVE-2005-1929 CVE-2005-1930	Medium	Security Focus, ID: 15867, 15868, December 14, 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 Mac OS X 10.3.9	A vulnerability has been reported in Perl due to a failure to correctly drop privileges, which could let a remote malicious user obtain elevated privileges. *Note: The impact depends on how a Perl application is written to use the affected Perl functionality.* No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Apple Mac OS X Perl Privilege Dropping CVE-2005-4217	Medium	Secunia Advisory: SA17922, December 13, 2005
CartKeeper CKGOLD	A Cross-Site Scripting vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'keywords' 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.	CKGold Cross-Site Scripting CVE-2005-4236	Medium	Secunia Advisory: SA17972, December 14, 2005
Daniel Stenberg curl 7.12-7.15, 7.11.2	A buffer overflow vulnerability has been reported due to insufficient bounds checks on user-supplied data before using in a finite sized buffer, which could let a local/remote malicious user execute	cURL / libcURL URL Parser Buffer Overflow CVE-2005-4077	High	Security Focus, Bugtraq ID: 15756, December 7, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:224,**

	arbitrary code. Upgrades available at: http://curl.haxx.se/download/curl-7.15.1.tar.gz **Mandriva:** **http://www.mandriva.com/security/advisories** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Debian:** **http://security.debian.org/pool/updates/main/c/curl/** Currently we are not aware of any exploits for this vulnerability.			**December 8, 2005** **Fedora Update Notifications, FEDORA-2005-1129 & 1130, December 8, 2005** **Debian Security Advisory, DSA 919-1, December 12, 2005**
DRZES HMS DRZES HMS 3.2	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'login.php' due to insufficient sanitization of user-supplied input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in the ' invoiceID' parameter due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	DRZES HMS Cross-Site Scripting &SQL Injection CVE-2005-4136 CVE-2005-4137	Medium	Security Focus, Bugtraq ID: 15766, December 7, 2005
Horde Project Mnemo 2.0.2	HTML injection vulnerabilities have been reported due to insufficient sanitization of the notepad name and other note data fields, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at:	Horde Mnemo Remote HTML Injection CVE-2005-4192	Medium	Security Focus, Bugtraq ID: 15803, December 12, 2005

	ftp://ftp.horde.org/pub/mnemo/mnemo-h3-2.0.3.tar.gz There is no exploit code required.			
Horde Project Turba Contact Manager 2.0.4	HTML injection vulnerabilities have been reported due to insufficient sanitization of the address book name and certain contact data fields, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://ftp.horde.org/pub/turba/turba-h3-2.0.5.tar.gz There is no exploit code required.	Horde Turba Multiple HTML Injection CVE-2005-4242	Medium	Security Focus, Bugtraq ID: 15802, December 12, 2005
Horde Project Horde Application Framework 3.0-3.0.7	HTML injection vulnerabilities have been reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/horde/horde-3.0.8.tar.gz There is no exploit code required.	Horde Application Framework HTML Injection CVE-2005-4190	Medium	Secunia Advisory: SA17970, December 12, 2005
Horde Project Kronolith 2.0.5, 2.0.4	HTML injection vulnerabilities have been reported due to insufficient sanitization of the calendar name and certain event data fields, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/kronolith/kronolith-h3-2.0.6.tar.gz There is no exploit code required.	Horde Kronolith HTML Injection CVE-2005-4189	Medium	Secunia Advisory: SA17971, December 12, 2005
Horde Project Nag 2.0-2.0.3, 1.1-1.1.3	HTML injection vulnerabilities have been reported due to insufficient sanitization of certain tasklist names and task	Horde Nag Remote HTML Injection	Medium	Security Focus, Bugtraq ID: 15804, December 12, 2005

	data fields, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/nag/nag-h3-2.0.4.tar.gz There is no exploit code required.	CVE-2005-4191		
IPsec-Tools IPsec-Tools0.6-0.6.2, 0.5-0.5.2	A remote Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions when in 'AGGRESSIVE' mode. Upgrades available at: http://prdownloads.sourceforge.net/ipsec-tools/ipsec-tools-0.6.3.tar.bz2?download Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/ipsec-tools/ **Gentoo: http://security.gentoo.org/glsa/glsa-200512-04.xml** Vulnerability can be reproduced with the PROTOS IPSec Test Suite.	IPsec-Tools ISAKMP IKE Remote Denial of Service CVE-2005-3732	Low	Security Focus, Bugtraq ID: 15523, November 22, 2005 Ubuntu Security Notice, USN-221-1, December 01, 2005 **Gentoo Linux Security Advisory, GLSA 200512-04, December 12, 2005**
Mike Neuman osh 1.7	A buffer overflow vulnerability has been reported in 'main.c' due to an error when handling environment variable substitutions, which could let a remote malicious user execute arbitrary with superuser privileges. **Debian: http://security.debian.org/pool/updates/main/o/osh/** There is no exploit code required; however a Proof of Concept exploit script has been published.	Mike Neuman OSH Remote Buffer Overflow CVE-2005-3346	High	Secunia Advisory: SA17527, November 9, 2005 **Debian Security Advisory, DSA 918-1, December 9, 2005**
Mike Neuman osh 1.7	A buffer overflow vulnerability exists in 'main.c' due to insufficient bounds checking in the 'iopen()' function, which could let a remote malicious	Mike Neuman OSH Command Line Argument Buffer Overflow	High	Secunia Advisory, SA14159, February 8, 2005 **Debian Security**

	user execute arbitrary code. **Debian:** **http://security.debian.org/pool/updates/main/o/osh/** An exploit script has been published.	CVE-2005-3533		**Advisory, DSA 918-1, December 9, 2005**
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'Install Trigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for a remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces,	Firefox Multiple Vulnerabilities CVE-2005-2260 CVE-2005-2261 CVE-2005-2262 CVE-2005-2263 CVE-2005-2264 CVE-2005-2265 CVE-2005-2267 CVE-2005-2269 CVE-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005

	which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-586.html Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/ http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/m		Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 Debian Security Advisory, DSA 779-1, August 20, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005 Slackware Security Advisory, SSA:2005-085-01, August 28, 2005 Debian Security Advisory, DSA 779-2, September 1, 2005 Debian Security Advisory, DSA 810-1, September 13, 2005 Fedora Legacy Update Advisory, FLSA:160202, September 14, 2005 HP Security Bulletin, HPSBOV01229, September 19, 2005 HP Security Bulletin, HPSBUX01230, October 3, 2005 Ubuntu Security Notice, USN-155-3, October 04, 2005

	/mozilla-firefox/ http://security.debian.org/pool/updates/main/m/mozilla/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-24.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ Debian: http://security.debian.org/pool/updates/main/m/mozilla/ Fedora: http://download.fedoralegacy.org/fedora/ HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBOV01229 HP: http://www.hp.com/products1/unix/java/mozilla/index.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-locale-da/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101952-1 SUSE: ftp://ftp.suse.com/pub/suse/ **Mandriva:**		Sun(sm) Alert Notification Sun Alert ID: 101952, October 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:226, December 12, 2005**

	http://www.mandriva.com/security/advisories Exploits have been published.			
Multiple Vendors Xpdf 3.0 pl2 & pl3, 3.0 1, 3.00, 2.0-2.03, 1.0 0, 1.0 0a, 0.90-0.93; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, 2.1, Enterprise Linux AS 4, AS 3, 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; teTeX 2.0.1, 2.0; Poppler poppler 0.4.2; KDE kpdf 0.5, KOffice 1.4.2 ; PDFTOHTML DFTOHTML 0.36	Multiple vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported in the 'DCTStream::read BaselineSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'DCTStream::read ProgressiveSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'StreamPredictor:: StreamPredictor()' function in 'xpdf/Stream.cc' when using the 'numComps' value to calculate the memory size, which could let a remote malicious user potentially execute arbitrary code; and a vulnerability was reported in the 'JPXStream: :readCodestream()' function in 'xpdf/JPXStream.cc' when using the 'nXTiles' and 'nYTiles' values from a PDF file to copy data from the file into allocated memory, which could let a remote malicious user potentially execute arbitrary code. Patches available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.01pl1.patch Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat:	Xpdf Buffer Overflows CVE-2005-3191 CVE-2005-3192 CVE-2005-3193	High	iDefense Security Advisory, December 5, 2005 Fedora Update Notifications, FEDORA-2005-1121 & 1122, December 6, 2005 RedHat Security Advisory, RHSA-2005:840-5, December 6, 2005 **KDE Security Advisory, advisory-20051207-1, December 7, 2005** **SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005** **Ubuntu Security Notice, USN-227-1, December 12, 2005**

	http://rhn.redhat.com/errata/RHSA-2005-840.html **KDE:** **ftp://ftp.kde.org/pub/kde/** **SUSE:** **ftp://ftp.suse.com/pub/suse/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Linux kernel 2.6-2.6.14	A Denial of Service vulnerability has been reported in 'net/ipv6/udp.c' due to an infinite loop error in the 'udp_v6_get_port()' function. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.tar.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPV6 Denial of Service CVE-2005-2973	Low	Secunia Advisory: SA17261, October 21, 2005 Fedora Update Notifications, FEDORA-2005-1007 & 1013, October 20, 2005 Security Focus, Bugtraq ID: 15156, October 31, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Linux kernel 2.6-2.6.15	An integer overflow vulnerability has been reported in 'INVALIDATE_INODE_PAGES2' which could lead to a Denial of Service and possibly execution of arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/	Linux Kernel Integer Overflow CVE-2005-3808	High	Fedora Update Notification, FEDORA-2005-1138, December 13, 2005

	linux/core/updates/4/ A Proof of Concept exploit script has been published.			
Multiple Vendors phpMyAdmin 2.7 .0-beta1, 2.6.4 -rc1, pl3, pl1, 2.6.3 -pl1, 2.6.2 -rc1, 2.6.2, 2.6.1 pl3, 2.6.1 pl1, 2.6.1 -rc1, 2.6.1, 2.6.0pl3, 2.6.0pl2, 2.6.0pl1, 2.5.7pl1, 2.5.7, 2.5.6 -rc1, 2.5.5 pl1, 2.5.5 -rc2, 2.5.5 -rc1, 2.5.5, phpMyAdmin phpMyAdmin 2.5 .0-2.5.4, 2.4.0, 2.3.2, 2.3.1, 2.2-2.2.6, 2.1-2.1 .2, 2.0- 2.0.5	Cross-Site Scripting vulnerabilities have been reported in the 'HTTP_HOST' variable and certain scripts in the libraries directory due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.7.0.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200512-03.xml** There is no exploit code required.	PHPMyAdmin Multiple Cross-Site Scripting CVE-2005-3665	Medium	phpMyAdmin security announcement PMASA-2005-8, December 5, 2005 **Gentoo Linux Security Advisory, GLSA 200512-03, December 12, 2005**
Multiple Vendors RedHat Enterprise Linux WS 3, ES 3, AS 3, Desktop 3.0; Linux kernel 2.4-2.4.28	A Denial of Service vulnerability has been reported in the 'find_target' function due to a failure to properly handle unexpected conditions when attempting to handle a NULL return value from another function. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.29.tar.bz2 RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **Debian:** **http://security.debian.org/pool/updates/main/k/** There is no exploit code required.	Linux Kernel Find_Target Local Denial of Service CVE-2005-2553	Low	Security Focus, Bugtraq ID: 14965, September 28, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **Debian Security Advisory. DSA 921-1, December 14, 2005**

Multiple Vendors SuSE Linux Enterprise Server 9, Linux 9.3 x86_64; Linux kernel 2.6.11, 2.6.8, 2.6.5	A vulnerability has been reported in 'ptrace' 64-bit platforms, which could let a malicious user access kernel memory pages. SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html Mandriva: http://www.mandriva.com/security/advisories **Debian: http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 64 Bit PTrace Kernel Memory Access CVE-2005-1763	Medium	SUSE Security Announcement, SUSE-SA:2005:029, June 9, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 Mandriva Linux Security Advisory, MDKSA-2005:220, November 30, 2005 **Debian Security Advisory, DSA 922-1, December 14, 2005**
Multiple Vendors SuSE Linux Professional 9.0, x86_64; Linux kernel 2.6-2.6.12, 2.5 .0- 2.5.69, 2.4-2.4.32	An unspecified Denial of Service vulnerability has been reported when stack fault exceptions are triggered. SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **Debian: http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Stack Fault Exceptions Denial of Service CVE-2005-1767	Low	Security Focus, 14467, August 3, 2005 SUSE Security Announce-ment, SUSE-SA:2005:044, August 4, 2005 Ubuntu Security Notice, USN-187-1, September 25, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **Debian Security Advisories, DSA 921-1 & 922-1, December 14, 2005**
Multiple Vendors SuSE Linux	A buffer overflow vulnerability has been reported in the XFRM network architecture code due	Linux Kernel XFRM Array Index Buffer	High	Security Focus, 14477, August 5, 2005

Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12	to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code. Patches available at: http://www.kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.	Overflow CVE-2005-2456		Ubuntu Security Notice, USN-169-1, August 19, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 200 Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005 **Debian Security Advisories, DSA 921-1 & 922-1, December 14, 2005**
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0, Linux Personal 10.0 OSS; Linux kernel 2.6-2.6.15	A Denial of Service vulnerability has been reported due to a race condition in 'do_coredump'. **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	Linux Kernel do_coredump Denial of Service CVE-2005-3527	Low	SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**

Multiple Vendors Trustix Secure Linux 2.2; Positive Software Corporation CP+ 2.5-2.5.4	A vulnerability has been reported in CP+ (cpplus), which potentially could let a remote malicious user cause a Denial of Service. Upgrades available at: http://cpplus.info/feature_25.html Trustix: http://http.trustix.org/pub/trustix/updates/ Currently we are not aware of any exploits for this vulnerability.	Positive Software Corporation CP+ Unspecified Perl Remote Denial of Service CVE-2005-4261	Low	Secunia Advisory: SA17975, December 12, 2005 Trustix Secure Linux Bugfix Advisory, 2005-0068, December 12, 2005
Multiple Vendors Trustix Secure Linux 3.0, 2.2, Secure Enterprise Linux 2.0, SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server for S/390 9.0, Linux Enterprise Server 9; 2.6-2.6.12.4	A Denial of Service vulnerability has been reported due to a failure to handle malformed compressed files. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.12.5.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories Mandriva: http://www.mandriva.com/security/advisories **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ZLib Null Pointer Dereference Denial of Service CVE-2005-2459	Low	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**

Multiple Vendors
 	
Ubuntu Linux 5.0 4 amd64, 4.1 ia64;
SuSE Linux 9.3 x86_64, 9.1 x86_64, 9.0 x86_64;
Linux kernel 2.6.10, 2.6.8
	A Denial of Service has been reported in 'ptrace()' due to insufficient validation of memory addresses.
	
	Updates available at:
	http://kernel.org/
	
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/
	
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-663.html
	
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-514.html
	
	Currently we are not aware of any exploits for this vulnerability.
		Linux Kernel 'ptrace()' Denial of Service
		
		CVE-2005-0756
			Low	Ubuntu Security Notice, USN-137-1, June 08, 2005
				
				SUSE Security Announcement, SUSE-SA:2005:029, June 9, 2005
				
				RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005
				
				RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005
				
				Debian Security Advisory, DSA 921-1, December 14, 2005

Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.12, 2.5.0-2.5.69, 2.4-2.4.32	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: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.11.12.tar.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Debian:** **http://security.debian.org/pool/updates/main/k/** There is no exploit code required.	Linux Kernel Network Bridge Information Disclosure CVE-2005-3272	Medium	Security Focus, Bugtraq ID: 15536, November 22, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 **Debian Security Advisory, DSA 922-1, December 14, 2005**

Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6.10, 2.6.8	A vulnerability was reported has been reported in the 'mmap()' function because memory maps can be created with a start address after the end address, which could let a malicious user cause a Denial of Service or potentially obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'MMap()' Denial of Service CVE-2005-1265	Medium	Ubuntu Security Notice, USN-137-1, June 08, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 **Debian Security Advisory, DSA 922-1, December 14, 2005**
Multiple Vendors Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha' Courier Mail Server 0.52.1, 0.47, 0.37.3	A vulnerability has been reported in the authentication daemon because access is granted to accounts that are already deactivated, which could let a remote malicious user obtain unauthorized access. Debian: http://security.debian.org/pool/updates/main/c/courier/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/courier/ There is no exploit code required.	Courier Mail Server Unauthorized Access CVE-2005-3532	Medium	Debian Security Advisory, DSA 917-1, December 8, 2005 Ubuntu Security Notice, USN-226-1, December 09, 2005
Multiple Vendors Linux Kernel 2.4, 2.6	A race condition vulnerability has been reported in ia32 emulation, that could let local malicious users obtain root privileges or create a buffer overflow. Patch Available: http://kernel.org/pub/	Linux Kernel Race Condition and Buffer Overflow CVE-2005-1768	High	Security Focus, 14205, July 11, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005 SUSE Security Announce-

	linux/kernel/v2.4/testing/patch-2.4.32-pre1.bz2 Trustix: http://http.trustix.org/pub/trustix/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.			ment, SUSE-SA:2005:044, August 4, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **Debian Security Advisory, DSA 921-1, December 14, 2005**
Multiple Vendors Linux kernel 2.6 prior to 2.6.12.1	A vulnerability has been reported in the 'restore_sigcontext()' function due to a failure to restrict access to the 'ar.rsc' register, which could let a malicious user cause a Denial of Service or obtain elevated privileges. Updates available at: http://www.kernel.org/ SUSE: http://www.novell.com/linux/security/advisories/2005_44_kernel.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of	Linux Kernel 64 Bit 'AR-RSC' Register Access CVE-2005-1761	Medium	Security Tracker Alert ID: 1014275, June 23, 2005 SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 **Debian Security Advisories, DSA 921-1 & 922-1, December 14, 2005**

	any exploits for this vulnerability.			
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in the '/sys' file system due to a mismanagement of integer signedness, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code. SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntupool/main/l/linux-source-2.6.8.1/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SYSFS_Write_ File Local Integer Overflow CVE-2005-0867	High	Security Focus, 13091, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 SUSE Security Announce-ment, SUSE-SA:2005:044, August 4, 2005 Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005 **Debian Security Advisory, DSA 922-1, December 14, 2005**
Multiple Vendors Linux Kernel 2.4.x, 2.6 prior to 2.6.11.11	A vulnerability has been reported in the Linux kernel in the Radionet Open Source Environment (ROSE) implementation in the 'rose_rt_ioctl()' function due to insufficient validation of a new routes' ndigis argument. The impact was not specified. Updates available at: http://linux.bkbits.net:8080/linux-2.4/cset@41e2cf515TpixcVQ8q8HvQvCv9E6zA Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/	Linux Kernel Radionet Open Source Environment (ROSE) ndigis Input Validation CVE-2005-3273	Not Specified	Security Tracker Alert, 1014115, June 7, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 **Debian Security Advisory, DSA 922-1, December 14, 2005** Mandriva Linux Security Advisories, MDKSA-2005:218, 219, & 220, November 30, 2005

	Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test11, 2.6.1-2.6.12; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3	A Denial of Service vulnerability has been reported on 64-bit platform due to a flaw in offset handling for the extended attribute file system code. RedHat: http://rhn.redhat.com/errata/RHSA-2005-294.html **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 64 Bit EXT3 Filesystem Extended Attribute Denial of Service CVE-2005-0757	Low	RedHat Security Advisory, RHSA-2005:294-29, May 18, 2005 **Debian Security Advisory, DSA 921-1, December 14, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6, -test9-CVS, -test1-test11, 2.6.1-2.6.9; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	A Denial of Service vulnerability has been reported in the 'fib_seq_start' function in 'fib_hash.c.' RedHat; http://rhn.redhat.com/errata/RHSA-2005-366.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Fib_Seq_Start' Denial of Service CVE-2005-1041	Low	RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**

Multiple Vendors Linux kernel 2.6.10-2.6.15	A Denial of Service vulnerability has been reported due to a memory leak in the kernel file lock lease code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.3.tar.bz2 SUSE: ftp://ftp.SUSE.com/pub/SUSE **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel File Lock Lease Local Denial of Service CVE-2005-3807	Low	SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005** **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A vulnerability has been reported in the EXT2/EXT3 file systems, which could let a remote malicious user bypass access controls. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2/EXT3 File Access Bypass CVE-2005-2801	Medium	Security Focus, Bugtraq ID: 14792, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 Mandriva Linux Security Advisory, MDKSA-2005:219, November 30, 2005 **Debian Security Advisory, DSA 921-1, December 14, 2005**

Multiple Vendors Linux kernel 2.6.8, 2.6.10	A remote Denial of Service vulnerability has been reported in the 'ipt_recent' module when specially crafted packets are sent. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html Mandriva: http://www.mandriva.com/security/advisories **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Ipt_recent' Remote Denial of Service CVE-2005-2872	Low	Security Focus, Bugtraq ID: 14791, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Linux kernel 2.6.8-2.6.10, 2.4.21	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'msg_control' when copying 32 bit contents, which could let a malicious user obtain root privileges and execute arbitrary code; and a vulnerability was reported in the 'raw_sendmsg()' function, which could let a malicious user obtain sensitive information or cause a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.	Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service CVE-2005-2490 CVE-2005-2492	High	Secunia Advisory: SA16747, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Fedora Update Notifications, FEDORA-2005-905 & 906, September 22, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 Mandriva Linux Security Update Advisory,

	redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html Mandriva: http://www.mandriva.com/security/advisories **SUSE: ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.			MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12 .3, 2.4-2.4.32	A Denial of Service vulnerability has been reported in 'IP_VS_CONN_FLUSH' due to a NULL pointer dereference. Kernel versions 2.6.13 and 2.4.32-pre2 are not affected by this issue. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories **Debian: http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Denial of Service CVE-2005-3274	Low	Security Focus, Bugtraq ID: 15528, November 22, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005 **Debian Security Advisory, DSA 922-1, December 14, 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/ Mandriva: http://www.mandriva.com/security/advisories **SUSE: ftp://ftp.suse.com/pub/suse/** 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 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Linux kernel 2.6-2.6.13.1	A Denial of Service vulnerability has been reported due to an omitted call to the 'sockfd_put()' function in the 32-bit compatible 'routing_ioctl()' function. Fixed version (2.6.13.2), available at: http://kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories **SUSE: ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel routing_ioctl() Denial of Service CVE-2005-3044	Low	Security Tracker Alert ID: 1014944, September 21, 2005 Ubuntu Security Notice, USN-187-1, September 25, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219, 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to a memory leak	Linux Kernel Denial of Service & Information	Medium	Secunia Advisory: SA17114, October 12, 2005

	in '/security/keys/request_key_auth.c;' a Denial of Service vulnerability was reported due to a memory leak in '/fs/namei.c' when the 'CONFIG_AUDITSYSCALL' option is enabled; and a vulnerability was reported because the orinoco wireless driver fails to pad data packets with zeroes when increasing the length, which could let a malicious user obtain sensitive information. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.14-rc4.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-808.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	Disclosure CVE-2005-3119 CVE-2005-3180 CVE-2005-3181		Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005 Fedora Update Notifications, FEDORA-2005-1013, October 20, 2005 RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported when handling asynchronous USB access via usbdevio; and a Denial of Service vulnerability was reported in the 'ipt_recent.c' netfilter module due to an error	Linux Kernel USB Subsystem Denials of Service CVE-2005-2873 CVE-2005-3055	Low	Secunia Advisory: SA16969, September 27, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005

	in jiffies comparison. RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.			Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Linux Kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in the 'sys_set_mempolicy' function when a malicious user submits a negative first argument; a Denial of Service vulnerability was reported when threads are sharing memory mapping via 'CLONE_VM'; a Denial of Service vulnerability was reported in 'fs/exec.c' when one thread is tracing another thread that shares the same memory map; a Denial of Service vulnerability was reported in 'mm/ioremap.c' when performing a lookup of a non-existent page; a Denial of Service vulnerability was reported in the HFS and HFS+ (hfsplus) modules; and a remote Denial of Service vulnerability was reported due to a race condition in 'ebtables.c' when running on a SMP system that is operating under a heavy load. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/	Multiple Vendors Linux Kernel Denials of Service CVE-2005-3053 CVE-2005-3106 CVE-2005-3107 CVE-2005-3108 CVE-2005-3109 CVE-2005-3110	Low	Ubuntu Security Notice, USN-199-1, October 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005 RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005 Mandriva Linux Security Advisories, MDKSA-2005: 219 & 220, November 30, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**

	Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-808.html Mandriva: http://www.mandriva.com/security/advisories **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Linux kernel 2.6-2.6.14, 2.5.0-2.5.69, 2.4-2.4.32, 2.3, 2.3.x, 2.3.99, pre1-pre7, 2.2-2.2.27, 2.1, 2.1.x, 2.1.89, 2.0.28-2.0.39	A vulnerability has been reported due to the way console keyboard mapping is handled, which could let a malicious user modify the console keymap to include scripted macro commands. Mandriva: http://www.mandriva.com/security/advisories **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/** There is no exploit code required; however, a Proof of Concept exploit has been published.	Linux Kernel Console Keymap Arbitrary Command Injection CVE-2005-3257	Medium	Security Focus, Bugtraq ID: 15122, October 17, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 **Fedora Update Notification, FEDORA-2005-1138, December 13, 2005**
Multiple Vendors Linux kernel 2.6-2.6.14; SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS; RedHat Fedora Core4	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	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 SuSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **SUSE Security**

	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.			**Announcement, SUSE-SA:2005:068, December 14, 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 **Trustix:** **http://http.trustix.org/pub/trustix/updates/** 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 **Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005**
Multiple Vendors Linux kernel 2.6-2.6.15; SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS; RedHat Fedora Core4	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 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE**	Linux Kernel PTraced Denial of Service CVE-2005-3784	Low	Security Focus, Bugtraq ID: 15625, November 29, 2005 Fedora Update Notification, FEDORA-2005-1104, November 28, 2005 SuSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005** **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**

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

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;
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
	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:
	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:
		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, 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
				Debian Security Advisor, DSA 919-1, December 12, 2005

	ftp://ftp.slackware.com/pub/slackware/ **Debian:** **http://security.debian.org/pool/updates/main/c/curl/** **Currently we are not aware of any exploits for this vulnerability.**			
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0 OSS; Linux kernel 2.6.10-2.6.14	A Denial of Service vulnerability has been reported due to a race condition error in the handling of POSIX timer cleanup routines. Linux kernel versions subsequent to 2.6.14 are not vulnerable to this issue. **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel POSIX Timer Cleanup Handling Local Denial of Service CVE-2005-3805	Low	SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0, Personal 10.0 OSS; Linux kernel 2.6-2.6.13, Linux kernel 2.4-2.4.32	A Denial of Service vulnerability has been reported in FlowLable. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.tar.bz2 **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPv6 FlowLable Denial of Service CVE-2005-3806	Low	Security Focus, Bugtraq ID: 15729, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Ubuntu Linux 4.1 ppc, ia64, ia32; Linux kernel 2.6.8, rc1&rc2	A remote Denial of Service vulnerability has been reported when handling UDP packets received by SNMPD due to a NULL pointer dereference. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/	Linux Kernel SNMP Handler Remote Denial of Service CVE-2005-2548	Low	Ubuntu Security Notice, USN-169-1, August 19, 2005 Mandriva Linux Security Advisory, MDKSA-2005:219, November 30, 2005 **Debian Security Advisory, DSA 922-1, December 14, 2005**

	advisories **Debian:** **http://security.debian.org/pool/updates/main/k/** Currently we are not aware of any exploits for this vulnerability.			
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/ Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.suse.com/pub/suse/ **Debian:** **http://security.debian.org/pool/updates/main/k/** 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 Mandriva Linux Security Advisories, MDKSA-2005:218 & 219, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 **Debian Security Advisory, DSA 922-1, December 14, 2005**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6.10, rc2, 2.6.8, rc1	A remote Denial of Service vulnerability has been reported in the kernel driver for compressed ISO file systems when attempting to mount a malicious compressed ISO image. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE**	Linux Kernel ISO File System Remote Denial of Service CVE-2005-2457	Low	Ubuntu Security Notice, USN-169-1, August 19, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005 **SUSE Security Announcement,**

	Mandriva: http://www.mandriva.com/security/advisories Currently we are not aware of any exploits for this vulnerability.			**SUSE-SA:2005:068, December 14, 2005**

Multiple Vendors
Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;
Trustix Secure Linux 3.0, 2.2,
Trustix Secure Enterprise Linux 2.0;
SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server 9;
Linux kernel 2.6-2.6.12 .4
	A Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions.
	Upgrades available at:
	http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.12.5.tar.gz
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/l/
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	Trustix:
	http://http.trustix.org/pub/trustix/updates/
	Mandriva:
	http://www.mandriva.com/security/advisories
	Mandriva:
	http://www.mandriva.com/security/advisories
	SUSE:
	ftp://ftp.suse.com/pub/suse/
	Currently we are not aware of any exploits for this vulnerability.
		Linux Kernel ZLib Invalid Memory Access Denial of Service
		CVE-2005-2458
			Low	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005
				Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005
				Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005
				SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005

Multiple Vendors Ubuntu Linux 5.0 4, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.13	A Denial of Service vulnerability has been reported in the '/proc/scsi/sg/devices' file due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.	Linux Kernel SCSI ProcFS Denial of Service CVE-2005-2800	Low	Security Focus, Bugtraq ID: 14790, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219, & 220, November 30,

	com/security/ advisories **SUSE:** **ftp://ftp.SUSE.com/ pub/SUSE** A Proof of Concept exploit has been published.			2005 **SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64; Linux kernel 2.6-2.6.12 .3	An information disclosure vulnerability has been reported in 'SYS_GET_THREAD _AREA,' which could let a malicious user obtain sensitive information. Kernel versions 2.6.12.4 and 2.6.13 are not affected by this issue. Ubuntu: http://security.ubuntu. com/ubuntu/pool/ main/l/ Mandriva: http://www.mandriva. com/security/ advisories **Debian:** **http://security.debian. org/pool/updates/ main/k/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Information Disclosure CVE-2005-3276	Medium	Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 **Debian Security Advisory, DSA 922-1, December 14, 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 'Perl_sv_ vcatpvfnl' 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. Webmin: http://prdownloads. sourceforge.net/ webadmin Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates OpenPKG: http://www.openpkg.	Perl 'miniserv.pl' script Format String CVE-2005-3912 CVE-2005-3962	Low	Security Focus, Bugtraq ID: 15629, November 29, 2005 Fedora Update Notifications, FEDORA-2005-1113, 1116, & 1117, December 1 & 2, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.025, December 3, 2005 Mandriva Linux Security Advisory, MDKSA-2005:223, December 2, 2005 Ubuntu Security Notice,

	org/security.html Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200512-01.xml http://security.gentoo.org/glsa/glsa-200512-02.xml **Mandriva: http://www.mandriva.com/security/advisories** **SUSE: ftp://ftp.suse.com/pub/suse/** **Trustix: http://http.trustix.org/pub/trustix/updates/** **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/perl/** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** An exploit has been published.			USN-222-1 December 02, 2005, December 2, 2005 Gentoo Linux Security Advisory, GLSA 200512-01 & 200512-02, December 7, 2005 US-CERT VU#948385 **Mandriva Linux Security Advisory, MDKSA-2005:225, December 8, 2005** **SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005** **Ubuntu Security Notice, USN-222-2, December 12, 2005** **Fedora Update Notifications, FEDORA-2005-1144 & 1145, December 14, 2005**
MySQL Auction MySQL Auction 3.0	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'keyword' 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.	MySQL Auction Cross-Site Scripting CVE-2005-4237	Medium	Secunia Advisory: SA18006, December 14, 2005

Openswan Openswan 2.2-2.4, 2.1.4-2.1.6, 2.1.2, 2.1.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported when handling IKE packets that have an invalid 3DES key length; and a remote Denial of Service vulnerability was reported when handling certain specially crafted IKE packets. Upgrades available at: http://www.openswan.org/download/openswan-2.4.2.tar.gz Astaro Security Linux: http://www.astaro.org/showflat.php?Cat=&Board=UBB1&Number=63678&Forum=All_Forums&Words=4.028&Searchpage=0&Limit=25&Main=63678&Search=true&where=bodysub&Name=&daterange=1&newerval=1&newertype=m&olderval=&oldertype=&bodyprev=#Post63678 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Gentoo: http://security.gentoo.org/glsa/glsa-200512-04.xml** Vulnerabilities can be reproduced using the PROTOS ISAKMP Test Suite.	Openswan IKE Message Remote Denials of Service CVE-2005-3671	Low	CERT-FI & NISCC Joint Vulnerability Advisory, November 15, 2005 Astaro Security Linux Update, November 16, 2005 Fedora Update Notifications, FEDORA-2005-1092 & 1093, November 21, 2005 **Gentoo Linux Security Advisory, GLSA 200512-04, December 12, 2005**
OpenVPN OpenVPN 2.0-2.0.2	Several vulnerabilities have been reported: a format string vulnerability was reported in 'options.c' when handling command options in the 'foreign_option()' function, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported due to a NULL pointer dereferencing error in the OpenVPN server when running in TCP mode.	OpenVPN Client Remote Format String & Denial of Service CVE-2005-3393 CVE-2005-3409	High	Secunia Advisory: SA17376, November 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.023, November 2, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Debian Security

	Updates available at: http://openvpn.net/download.html OpenPKG: ftp://ftp.openpkg.org/release/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/o/openvpn/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-07.xml Mandriva: http://www.mandriva.com/security/advisories **Mandriva: http://www.mandriva.com/security/advisories** Cu**rrently we are not aware of any exploits for these vulnerabilities**.			Advisory, DSA 885-1, November 7, 2005 Gentoo Linux Security Advisory, GLSA 200511-07, November 7, 2005 Mandriva Linux Security Advisory, MDKSA-2005:206, November 8, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:206-1, December 9, 2005**
phpMyAdmin phpMyAdmin 2.7.0-beta1, 2.7	A vulnerability has been reported in the register_globals emulation layer in 'grab_globals.php' because the 'import_blacklist' variable is not properly protected, which could let a remote malicious user execute arbitrary HTML and script code and include arbitrary files. Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.7.0-pl1.tar .gz **Gentoo: http://security.gentoo.org/glsa/glsa-200512-03.xml** There is no exploit code required.	PHPMyAdmin 'Import_Blacklist' Variable Overwrite CVE-2005-4079	Medium	Secunia Advisory: SA17925, December 7, 2005 **Gentoo Linux Security Advisory, GLSA 200512-03, December 12, 2005**

SCO Unixware 7.1.4, 7.1.3	A buffer overflow vulnerability has been reported in 'UIDAdmin' when processing excessive data, which could let a malicious user obtain superuser privileges. Updates available at: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.54/SCOSA-2005.54.txt Currently we are not aware of any exploits for this vulnerability.	SCO UnixWare Buffer Overflow CVE-2005-3903	High	SCO Security Advisory, SCOSA-2005.54, December 12, 2005
Scout Portal Toolkit Scout Portal Toolkit 1.3.1	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of user-supplied input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient sanitization of 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; however, Proofs of Concept exploit scripts have been published.	Scout Portal Toolkit Cross-Site Scripting & SQL Injection CVE-2005-4195 CVE-2005-4196	Medium	Security Focus, Bugtraq ID: 15818, December 12, 2005
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0	A vulnerability has been reported when running Sun Update Connection Services due to an unspecified error which could let a malicious user obtain knowledge of the configured web proxy password. Patches available: http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102090-1 There is no exploit code required.	Sun Solaris Sun Update Connection Web Proxy Password Disclosure CVE-2005-4133	Medium	Sun(sm) Alert Notification Sun Alert ID: 102090, December 7, 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/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-848.html http://rhn.redhat.com/errata/RHSA-2005-850.html **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/**	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 RedHat Security Advisory, RHSA-2005:848-6 & 850-5, December 6, 2005 Fedora Update Notifications, FEDORA-2005-1112 & 1115, December 8, 2005

	Currently we are not aware of any exploits for this vulnerability.			
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/ Debian: http://security.debian.org/pool/updates/main/z/zope2.7/ **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zope2.8/** Currently we are not aware of any exploits for this vulnerability.	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 **Ubuntu Security Notice, USN-229-1, December 13, 2005**

[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
Acme Software PerlCal 2.99.30, 2.99.20, 2.99	A Cross-Site Scripting vulnerability has been reported in 'Cal_make.PL' due to insufficient sanitization of the 'p0' parameter before displaying input, which could let a remote malicious user execute arbitrary	ACME Perl-Cal Cross-Site Scripting CVE-2005-4162	Medium	Security Tracker Alert ID: 1015332, December 8, 2005

	HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.			
Apache Software Foundation James 2.2	A remote Denial of Service vulnerability has been reported due to an error condition in the spooler. The vendor has addressed this issue in the CVS. Users are advised to contact the vendor for further information. Currently we are not aware of any exploits for this vulnerability.	Apache James Spooler Memory Leak Remote Denial of Service CVE-2004-2650	Low	Security Focus, Bugtraq ID: 15765, December 7, 2005
Apache Software Foundation Apache prior to 1.3.35-dev, 2.0.56-dev	A Cross-Site Scripting vulnerability has been reported in the 'Referer' directive in 'mod_imap' due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. The vulnerability has been fixed in version 1.3.35-dev, and 2.0.56-dev. OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.029-apache.html There is no exploit code required.	Apache mod_imap Cross-Site Scripting CVE-2005-3352	Medium	Security Tracker Alert ID: 1015344, December 13, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.029, December 14, 2005
Apani Networks Corporation EpiForce Agent 1.9 & prior	A remote Denial of Service vulnerability has been reported due to insufficient validation of Internet Key Exchange (IKE) packets. The vendor has released version 2.0 to address this issue. There is no exploit code required.	Apani Networks EpiForce IPSec IKE Processing Remote Denial of Service CVE-2005-3670	Low	Security Tracker Alert ID: 1015340, December 11, 2005
Arab Portal System Arab Portal System 2.0 beta 2	An SQL injection vulnerability has been reported in 'link.php' due to insufficient sanitization of the 'PHPSESSID' 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	Arab Portal SQL Injection CVE-2005-4221	Medium	Secunia Advisory: SA17984, December 13, 2005

	script has been published.			
Blackboard Blackboard Academic Suite 6.0	A Cross-Domain vulnerability has been reported in 'frameset.jsp' due to a design error, which could let a remote malicious user obtain sensitive information or hijack sessions. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Blackboard Academic Suite Cross-Domain CVE-2005-4206	Medium	Secunia Advisory: SA17991, December 12, 2005
CFMagic Magic List Professional 2.5, Magic Forum Personal 2.5, Magic Book Professional 2.0	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML, script code, and 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.	CFMagic Multiple Products Input Validation CVE-2005-4071 CVE-2005-4072 CVE-2005-4073	Medium	Security Focus, Bugtraq ID: 15774, December 8, 2005
CFMagic Magic Book Professional 2.0	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'StartRow' parameter before returning 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.	Magic Book Professional Cross-Site Scripting CVE-2005-4177	Medium	Secunia Advisory: SA17982, December 12, 2005
Computer Associates CleverPath Portal 4.7	A Cross-Site Scripting vulnerability has been reported in the login page due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=QI70871 There is no exploit code required.	CA CleverPath Portal Cross-Site Scripting CVE-2005-4150	Medium	Secunia Advisory: SA17962, December 9,2005

Contenido Contenido 4.6.1, 4.6	A vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.contenido.org/opensourcecms/de/upload/versionen/contenido-4 .6.4.zip There is no exploit code required.	Contenido CMS Remote Command Execution CVE-2005-4132	Medium	Security Focus, Bugtraq ID: 15790, December 9,2005
CourseForum Technologies ProjectForum 4.7	Cross-Site Scripting vulnerabilities have been reported in various pages and error messages due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a remote Denial of Service vulnerability has been reported in the 'pageid' parameter due to a boundary error when sending a POST request. 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.	CourseForum Technologies ProjectForum Cross-Site Scripting & Denial of Service	Medium	Security Focus, Bugtraq ID: 15850, December 14, 2005
Dell TrueMobile 2300 Firmware 5.1.1 .6, 3.0.08	A vulnerability has been reported in the 'apply.cgi' page of the router's web management interface due to an access control error, which could let a remote malicious user bypass authentication. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Dell TrueMobile 2300 Remote Authentication Bypass CVE-2005-3661	Medium	iDEFENSE Labs Security Advisories, December 7, 2005
DoceboLMS DoceboLMS 2.0.4	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in the 'connector.php' script due to insufficient validation of the 'Type' parameter, which could let a remote malicious user obtain sensitive information; and an input validation vulnerability was reported in the file upload handling due to insufficient verification of the file extension of valid images, which could let a remote malicious user execute arbitrary PHP code.	DoceboLMS Directory Traversal & File Upload CVE-2005-4094 CVE-2005-4095	High	Security Tracker Alert ID: 1015308, December 5, 2005 **Security Focus, Bugtraq ID: 15744 & 15742, December 13, 2005**

	Upgrades available at: **http://www.docebolms.org/download.php?type=docs&pb=395&id=48** **http://www.docebolms.org/download.php?type=docs&pb=321&id=49** There is no exploit code required; however, a Proof of Concept exploit script has been published.			
DreamLevels Dream Poll 3.0 final	An SQL injection vulnerability has been reported in 'view_results.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 script has been published.	DreamLevels Dream Poll SQL Injection CVE-2005-4254	Medium	Security Focus, Bugtraq ID: 15849, December 14, 2005
Envolution Software Envolution	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the News module due to insufficient filtering of HTML code, which could let a remote malicious user execute arbitrary scripting code; and an SQL injection vulnerability was reported when a remote malicious user submits specially crafted parameter values, which could lead to the execution of arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit scripts have been published.	Envolution SQL Injection & Cross-Site Scripting CVE-2005-4262 CVE-2005-4263	Medium	Security Tracker Alert ID: 1015351, December 13, 2005

Ethereal Group Ethereal 0.10-0.10.13, 0.9-0.9.16, 0.8.19, 0.8.18, 0.8.13-0.8.15, 0.8.5, 0.8, 0.7.7	A buffer overflow vulnerability has been reported in the 'dissect_ospf_v3_address_prefix()' function in the OSPF protocol dissector due to a boundary error when converting received binary data to a human readable string, which could let a remote malicious user execute arbitrary code. Patch available at: http://anonsvn.ethereal.com/viewcvs/viewcvs.py/trunk/epan/dissectors/packet-ospf.c?rev=16507&view=markup Debian: http://security.debian.org/pool/updates/main/e/ethereal/ Gentoo: http://security.gentoo.org/glsa/glsa-200512-06.xml Currently we are not aware of any exploits for this vulnerability.	Ethereal OSPF Protocol Dissection Buffer Overflow CVE-2005-3651	High	iDefense Security Advisory, December 9, 2005 Debian Security Advisory DSA 920-1, December 13, 2005 Gentoo Linux Security Advisory, GLSA 200512-06, December 14, 2005
EveryAuction EveryAuction 1.53	A Cross-Site Scripting vulnerability has been reported in 'auction.pl' due to insufficient sanitization of the 'searchstring' parameter before returning to the user, 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.	EveryAuction Cross-Site Scripting CVE-2005-4229	Medium	Security Focus, Bugtraq ID: 15824, December 13, 2005
FFmpeg FFmpeg 0.4.9 -pre1, 0.4.6-0.4.8, FFmpeg CVS	A buffer overflow vulnerability has been reported in the 'avcodec_default_get_buffer()' function of 'utils.c' in libavcodec due to a boundary error, which could let a remote malicious user execute arbitrary code. Patches available at: http://www1.mplayerhq.hu/cgi-bin/cvsweb.cgi/ffmpeg/libavcodec/utils.c.diff?cvsroot=FFMpeg&r2=1.162&r1=1.161&f=u **Ubuntu:**	FFmpeg Remote Buffer Overflow CVE-2005-4048	High	Secunia Advisory: SA17892, December 6, 2005 **Ubuntu Security Notice, USN-230-1, December 14, 2005**

	http://security.ubuntu.com/ubuntu/pool/main/f/ffmpeg/ Currently we are not aware of any exploits for this vulnerability.			
First4Internet CodeSupport	A vulnerability has been reported due to a failure to verify that the source of remote content is from a trusted source before downloading, which could let a remote malicious user execute arbitrary code. **Microsoft:** **http://www.microsoft.com/technet/security/Bulletin/MS05-054.mspx** There is no exploit code required.	First 4 Internet CodeSupport Remote Arbitrary Code Execution CVE-2005-3650	High	Security Focus, Bugtraq ID: 15430, November 15, 2005 US-CERT VU#312073 **Microsoft Security Bulletin MS05-054, December 13, 2005**
FlatNuke FlatNuke 2.5.6	A vulnerability has been reported in the 'read' module due to insufficient validation of the 'id' parameter, which could let a remote malicious user obtain elevated privileges and execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Flatnuke Elevated Privileges & Remote Command Execution CVE-2005-4208	High	Security Tracker Alert ID: 1015339, December 11, 2005
Francisco Burzi PHP-Nuke 7.6-7.9, 7.0-7.3	A content filtering bypass vulnerability has been reported which could let a remote malicious user bypass filters and carry out HTML injection and Cross-Site Scripting attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit scripts have been published.	PHPNuke Content Filtering Bypass CVE-2005-4260	Medium	Security Focus, Bugtraq ID: 15855, December 14, 2005
Hewlett Packard Company OpenView Network Node Manager 7.50 Solaris, 7.50, 6.41 Solaris, 6.41	A vulnerability has been reported in the 'node' URI parameter of the 'OvCgi/connectedNodes.ovpl' script, which could let a remote malicious user execute arbitrary code. Revision 3: Added PHSS_33783. Added preliminary files for OV NNM 7.01, 6.4, 6.2 Revision 4: Corrected files are available via ftp:	HP OpenView Network Node Manager Remote Arbitrary Code Execution CVE-2005-2773	High	Portcullis Security Advisory, 05-014, August 25, 2005 HP Security Advisory, HPSBMA01224, August 26, 2005 HP Security Advisory, HPSBMA01224 REVISION: 3, September 13, 2005

	README_HPSBMA01224_rev1.txt NNM6.2_HP-UX_CGI_Script_Point_Release_rev1.tar NNM6.2_HP-UX_CGI_Script_Point_Release_rev1.tar Revision 5: Added PHSS_33842, PSOV_03430, and NNM_01110. Changed revision numbering (6.20, 6.4x instead of 6.2,6.4, 6.40, 6.41). Workaround available at: http://support.openview.hp.com/news_archives.jsp **Another exploit script has been published.**			HP Security Advisory, HPSBMA01224 REVISION: 4, September 19, 2005 HP Security Advisory, HPSBMA01224 REVISION: 5, October 4, 2005 **Security Focus, Bugtraq ID: 14662, December 8, 2005**
Jamit Software Job Board 2.4.1	An SQL injection vulnerability has been reported in 'index.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. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Jamit Job Board SQL Injection [CVE-2005-4232](CVE-2005-4232)	Medium	Secunia Advisory: SA18007, December 14, 2005
Lars Ellingsen Guestserver 5.0	A HTML injection vulnerability has been reported in 'GuestServer.cgi' due to insufficient sanitization before using in dynamically generated content, 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.	Guestserver HTML Injection [CVE-2005-4222](CVE-2005-4222)	Medium	Security Focus, Bugtraq ID: 15821, December 12, 2005
Linksys WRT54GS 4.70.6 (Firmware), 4.50.6 (Firmware), BEFW11S4 v4, BEFW11S4 v3, BEFW11S4 1.44, 1.43.3, 1.4.3, 1.4.2 .7	A remote Denial of Service vulnerability has been reported when handling TCP 'LanD' packets. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit scrip has been published.	Multiple Linksys Routers Remote Denial of Service [CVE-2005-4257](CVE-2005-4257)	Low	Security Focus, Bugtraq ID: 15861, December 14, 2005

Lyris List Manager 8.8 a, 8.0, 7.0, 6.0, 5.0	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'pw' parameter in the web interface when subscribing a new user to the mailing list due to insufficient sanitization before inserting in the processing queue as a command message, which could let a remote malicious user execute arbitrary list administration commands; an SQL query vulnerability was reported in '/read/attachment' due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; an SQL vulnerability was reported in certain parameters due to insufficient sanitization before used as a column name to the ORDER BY command in a SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in the MSDE version of ListManager because a weak default password is used for the database after installation, which could let a remote malicious user obtain sensitive information; a vulnerability was reported because certain versions allow access to the 'status' module of the 'TCLHTTPd' service, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in the 'TCLHTTPd' service because the source of arbitrary TML scripts on the server can be viewed; and a vulnerability was reported because the entire CGI environment is included into a HTML hidden variable of the error page when a non-existent page is requested. Some of these vulnerabilities have reportedly been fixed in version 8.9b. There is no exploit code required.	Lyris ListManager Multiple Vulnerabilities CVE-2005-4142 CVE-2005-4143 CVE-2005-4144 CVE-2005-4145 CVE-2005-4146 CVE-2005-4147 CVE-2005-4148 CVE-2005-4149	Medium	Secunia Advisory: SA17943, December 9, 2005
Macromedia Flash Media Server Professional Edition 2.0, Flash Media Server Origin	A Denial of Service vulnerability has been reported due to an error in the Administration Service (FMSAdmin.exe) when handling received data. No workaround or patch available at time of publishing.	Macromedia Flash Media Server Administration Service Denial of Service	Low	Security Focus, Bugtraq ID: 15822, December 13, 2005

Edition 2.0, Flash Media Server Edge Edition 2.0, Flash Media Server Developer Edition 2.0	There is no exploit code required; however, a Proof of Concept exploit has been published.	CVE-2005-4216		
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. **Joomla:** **http://developer.joomla.org/sf/frs/do/viewRelease/projects.joomla/frs.joomla_1_0.1_0_4** An exploit script has been published. Reports indicate that a bot is propagating in the wild by exploiting this vulnerability.	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 Security Focus, Bugtraq ID: 15461, December 5, 2005 **Security Focus, Bugtraq ID: 15461, December 9, 2005**
Mantis Mantis 1.x	A Cross-Site Scripting vulnerability has been reported in 'view_filters_page.php' due to insufficient sanitization of the 'target_field' 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 script has been published.	Mantis Cross-Site Scripting CVE-2005-4238	Medium	Secunia Advisory: SA18018, December 14, 2005
McGallery McGallery 2.2, 1.1, 1.0	Several vulnerabilities have been reported: a vulnerability was reported in 'index.php' due to insufficient verification of the 'language' parameter before used to include files, which could let a remote malicious users include arbitrary files; a vulnerability was reported in 'show.php' due to insufficient sanitization of the 'id,'	mcGalleryPRO Multiple Vulnerabilities CVE-2005-4250 CVE-2005-4251 CVE-2005-4252	Medium	Security Focus, Bugtraq ID: 15845, December 14, 2005

	'rand,' and 'start' parameters and in 'index.php' due to insufficient sanitization of the 'album' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of certain parameters 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; however, Proof of Concept exploit scripts have been published.			
MediaWiki MediaWiki 1.5 alpha1&2, bet1-beta3, 1.4-1.4.10, 1.3.13, 1.3-1.3.11	A Cross-Site Scripting vulnerability has been reported in inline style attributes due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/wikipedia/mediawiki-1.4.12.tar.gz?download **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	MediaWiki HTML Inline Style Attributes Cross-Site Scripting CVE-2005-3167	Medium	Security Focus, Bugtraq ID: 15024, October 6, 2005 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 **SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005**
MilliScripts MilliScripts 1.4	A Cross-Site Scripting vulnerability has been reported in 'register.php' due to insufficient sanitization of the 'domainname' 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 script has been published.	Milliscripts Cross-Site Scripting CVE-2005-4161	Medium	Secunia Advisory: SA17997, December 12, 2005
Motorola Motorola Cable Modem SB5100E	A remote Denial of Service vulnerability has been reported when handling TCP 'LanD' packets. No workaround or patch available at	Motorola SB5100E Cable Modem Remote Denial of Service	Low	Security Focus, Bugtraq ID: 15795, December 9, 2005

	time of publishing. There is no exploit code required.	CVE-2005-4215		
Mozilla Firefox 1.5, Netscape Browser 8.0.4; Netscape Browser 8.0.4	A remote Denial of Service vulnerability has been reported when handling large history information. *Note: The vendor disputes this claim.* No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Mozilla History File Remote Denial of Service CVE-2005-4134	Low	Secunia Advisory: SA17934, December 8, 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/ OpenPKG: http://www.openpkg.org/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** 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 OpenPKG Security Advisory, OpenPKG-SA-2005.027, December 3, 2005 **SuSE Security Announcement, SUSE-SA:2005:069, December 14, 2005**

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	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, 2005 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

	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/ 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		Security Focus, Bugtraq ID: 14088, November 7, 2005 Security Focus, Bugtraq ID: 14088, November 23, 2005 **HP Security Bulletin, HPSBTU02083, December 9, 2005**

	-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 **HP:** **http://www.securityfocus.com/advisories/9831** Exploit scripts have been published.			
MyBB Group MyBulletinBoard 1.0 PR2, RC1-RC4	Several vulnerabilities have been reported: SQL injection vulnerabilities were reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and unspecified vulnerabilities were reported which could compromise a vulnerable MyBB installation. Upgrades available at: http://www.mybboard.com/downloads/?action=request&did=13&type=zip Currently we are not aware of any exploits for these vulnerabilities.	MyBB SQL Injection & Unspecified Vulnerabilities CVE-2005-4199 CVE-2005-4200	Medium	TKPN2005-12-001, December 9, 2005
NetGear RP114 3.26	A remote Denial of Service vulnerability has been reported when a malicious user initiates a TCP SYN flood to the external interface of the device. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	NetGear RP114 SYN Flood Denial of Service CVE-2005-4220	Low	Securiteam Advisory, December 13, 2005

Netref Netref 3.0	An SQL injection vulnerability has been reported in 'index.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. There is no exploit code required.	Netref SQL Injection Scripting CVE-2005-4198	Medium	Security Focus, Bugtraq ID: 15801, December 12, 2005
Nortel Networks SSL VPN 4.2.1.6	A vulnerability has been reported in 'tunnelform.yaws' due to insufficient sanitization of the 'a' 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 script has been published.	Nortel SSL VPN Web Interface Input Validation CVE-2005-4197	Medium	SEC-CONSULT Security Advisory 20051212-0, December 10, 2005

OpenSSH OpenSSH 4.1, 4.0, p1	Several vulnerabilities have been reported: a vulnerability was reported due to an error when handling dynamic port forwarding when no listen address is specified, which could let a remote malicious user cause "GatewayPorts" to be incorrectly activated; and a vulnerability was reported due to an error when handling GSSAPI credential delegation, which could let a remote malicious user be delegated with GSSAPI credentials. Upgrades available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-4.2.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-527.html Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/openssh/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **SCO:**	OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials CVE-2005-2797 CVE-2005-2798	Medium	Secunia Advisory: SA16686, September 2, 2005 Fedora Update Notification, FEDORA-2005-858, September 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 Slackware Security Advisory, SSA:2005-251-03, September 9, 2005 Fedora Update Notification, FEDORA-2005-860, September 12, 2005 RedHat Security Advisory, RHSA-2005:527-16, October 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:172, October 6, 2005 Ubuntu Security Notice, USN-209-1, October 17, 2005 Conectiva Linux Announcement, CLSA-2005:1039, October 19, 2005 **SCO Security Advisory, SCOSA-2005.53, December 12, 2005**

	ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.53 There is no exploit code required.			
Opera Software Opera Web Browser 8.50, 8.0-8.0 2	A remote Denial of Service vulnerability has been reported when handling large page titles due to an error. Upgrades available at: http://www.opera.com/download/ There is no exploit code required.	Opera Web Browser Long Page Title Remote Denial of Service CVE-2005-4210	Low	Opera Software Advisory, December 12, 2005
PGP Corporation PGP Desktop Professional 9.0.3 Build 2932, 9.0 PGP Desktop Home 8.0	A vulnerability has been reported when using the Wipe Free Space tool because data contained in the slack space of files on a NTFS drive is not correctly wiped, which could lead to the disclosure of sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, the Slacker tool may be used to exploit this vulnerability.	PGP Desktop Wipe Free Space Assistant Improper Disk Wipe CVE-2005-4151	Medium	Metasploit Project Advisory, December 8,2005
PHP JackKnife PHP JackKnife 2.21	A Cross-Site Scripting vulnerability has been reported in 'DisplayResults.php' due to insufficient sanitization of the 'sKeywords 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 exploit scripts have been published.	PHP JackKnife Gallery System Cross-Site Scripting CVE-2005-4239	Medium	Security Focus, Bugtraq ID: 15841, December 13, 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	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

	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 **SUSE:** **ftp://ftp.suse.com/pub/suse/** Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ OpenPKG:		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 OpenPKG Security Advisory, OpenPKG-SA-2005.027, December 3, 2005 **SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005** **SUSE Security Announcement, SUSE-SA:2005:069, December 14, 2005**

	http://www.openpkg.org/ There is no exploit code required.			
PHP Web Scripts Ad Manager Pro 2.0	An SQL injection vulnerability has been reported in 'Advertiser_statistic.php' 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; however, a Proof of Concept exploit script has been published.	PHP Web Scripts Ad Manager Pro SQL Injection CVE-2005-4233	Medium	Security Focus, Bugtraq ID: 15847, December 14, 2005
PHP Web Scripts Link Up Gold 2.5	Cross-Site Scripting vulnerabilities have been reported in 'tell_friend.php' due to insufficient sanitization of the 'link' parameter and in 'search.php' due to insufficient sanitization of the 'phrase[0]' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Link Up Gold Cross-Site Scripting CVE-2005-4230 CVE-2005-4231	Medium	Security Focus, Bugtraq ID: 15843, December 13, 2005
phpCOIN phpCOIN 1.2.2	A Cross-Site Scripting vulnerability has been reported in 'Coin_CFG.php' due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPCoin SQL Injection CVE-2005-4213	Medium	Security Focus, Bugtraq ID: 15830, December 13, 2005
phpCOIN phpCOIN 1.2.2	A file include vulnerability has been reported in 'config.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;	PHPCoin File Include CVE-2005-4212	High	Security Focus, Bugtraq ID: 15831, December 13, 2005

	however, a Proof of Concept exploit script has been published.			
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 **SUSE:** **ftp://ftp.suse.com/pub/suse/** 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 **SUSE Security Announcement, SUSE-SA:2005:069, December 14, 2005**
PhpWeb Gallery PhpWebGallery 1.5.1	SQL injection vulnerabilities have been reported in 'comments.php' due to insufficient sanitization of the 'sort_by' and 'items_number' parameters and in 'picture.php' due to insufficient sanitization of the 'image_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL. 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.	PHPWebGallery SQL Injection CVE-2005-4228	Medium	Security Focus, Bugtraq ID: 15837, December 13, 2005
Plogger Plogger Beta 2	Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient of the 'page' and 'id' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'level' and 'searchterms' parameters 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 script has been published.	Plogger SQL Injection & Cross-Site Scripting CVE-2005-4246 CVE-2005-4247	Medium	Security Focus, Bugtraq ID: 15839, December 13, 2005

PowerDev EncapsGallery 1.0	An SQL injection vulnerability has been reported in 'gallery.php' due to insufficient sanitization of the '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 script has been published.	EncapsGallery SQL Injection CVE-2005-4234	Medium	Security Focus, Bugtraq ID: 15836, December 13, 2005
QNX Software Systems Ltd. RTOS 4.25	A vulnerability has been reported in the 'dhcp.client' program because it has suid root permissions, which could let a remote malicious user change the assigned IP addresses of network interfaces and potentially cause a Denial of Service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	QNX RTOS 'dhcp.client' File Permission CVE-2005-4082	Low	Security Focus, Bugtraq ID: 15785, December 9, 2005
Simple Machines SMF 1.1 rc1	An SQL injection vulnerability has been reported in 'memberlist.php' 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; however, a Proof of Concept exploit script has been published.	Simple Machines Forum SQL Injection CVE-2005-4159	Medium	KAPDA Advisory #16, December 9, 2005
SimpleMedia SimpleBBS 1.1, 1.0.7, 1.0.6	A vulnerability has been reported in the 'name' parameter when adding a new topic due to insufficient sanitization, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	SimpleBBS Input Validation CVE-2005-4135	High	Security Tracker Alert ID: 1015323, December 7, 2005
Snipe Gallery Snipe Gallery 3.1.4	Several vulnerabilities have been reported: SQL injection vulnerabilities were reported in 'image.php' due to insufficient sanitization of the 'image_id'	Snipe Gallery Cross-Site Scripting & SQL Injection	Medium	Secunia Advisory: SA18022, December 14, 2005

	parameter and in 'view.php' due to insufficient sanitization of the 'gallery_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 'keyword' 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 exploit scripts have been published.	CVE-2005-4244 CVE-2005-4245		
ThWb Group Thwboard Beta 2.8	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user inject arbitrary HTML, script code, or SQL code. Upgrade available at: http://prdownloads.sourceforge.net/thwb/thwb-300-beta-2.84-php5.tar.gz There is no exploit code required; however, Proof of Concept exploits have been published.	ThWboard Multiple Input Validation CVE-2005-4138 CVE-2005-4139	Medium	KAPDA Advisory #15, December 7, 2005
Triangle Solutions Ltd. PHP Support Tickets 2.0	SQL injection vulnerabilities have been reported in the login page due to insufficient validation of the 'username' and password' fields and in 'index.php' due to insufficient verification of the 'id' parameter, which could let a remote malicious user execute arbitrary SQL code. Update available at: http://www.phpsupporttickets.com/ There is no exploit code required.	PHP Support Tickets Multiple SQL Injection CVE-2005-4264	Medium	Security Tracker Alert ID: 1015352, December 13, 2005

UseBB UseBB 0.6 a, 0.6, 0.5.1 a, 0.5.1	A Cross-Site Scripting vulnerability has been reported in '$_SERVER['PHP_SELF']' due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/usebb/usebb-0.7.tar.gz?download There is no exploit code required.	UseBB Cross-Site Scripting CVE-2005-4193	Medium	Secunia Advisory: SA17958, December 12, 2005
VCD-db VCD-db 0.971-0.973, 0.961, 0.98, 0.97	Several vulnerabilities have been reported: a Cross-Site vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'batch' parameter and when performing a detailed search due to insufficient sanitization of the 'title' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because it is possible to obtain the full path to 'search.php' when accessed by an invalid 'by' parameter. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit scripts have been published.	VCD-db Cross-Site Scripting & Path Disclosure CVE-2005-4240 CVE-2005-4241	Medium	Secunia Advisory: SA18034, December 14, 2005
Website Baker Project Website Baker 2.6, 2.5.2	An SQL injection vulnerability has been 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. Upgrades available at: http://download.websitebaker.org/websitebaker2/stable/2.6.1/websitebaker-2.6.1.tar.gz/ There is no exploit code required; however, a Proof of Concept exploit script has been published.	Website Baker SQL Injection CVE-2005-4140	Medium	Security Focus, Bugtraq ID: 15776, December 12, 2005
WHM Complete Solution WHMComplete Solution 2.1	A Cross-Site Scripting vulnerability has been reported in 'knowledgebase.php' due to insufficient sanitization of the 'search' parameter before returning to the user, which could let a remote	WHMComplete Solution Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 15856, December 14, 2005

	malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	CVE-2005-4235		
WikkaWiki WikkaWiki 1.1.6.0	A Cross-Site Scripting vulnerability has been reported in 'TextSearch.PHP' due to insufficient sanitization of the 'phrase' 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 scrip has been published.	WikkaWiki Cross-Site Scripting CVE-2005-4255	Medium	Secunia Advisory: SA18015, December 14, 2005
XMail XMail 1.21	A buffer overflow vulnerability has been reported in the 'AddressFromAtPtr()' function due to a boundary error when copying the hostname portion of an e-mail address to a 256-byte buffer, which could let a malicious user execute arbitrary code. Upgrade available at: http://www.xmailserver.org/ Debian: http://security.debian.org/pool/updates/main/x/xmail/ **Gentoo: http://security.gentoo.org/glsa/glsa-200512-05.xml** An exploit script has been published.	XMail Command Line Buffer Overflow CVE-2005-2943	High	Security Tracker Alert ID: 1015055, October 13, 2005 Security Focus, Bugtraq ID: 15103, October 22, 2005 Debian Security Advisory, DSA 902-1, November 21, 2005 **Gentoo Linux Security Advisory, GLSA 200512-05, December 14, 2005**

[back to top]

Wireless

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

- **Bluetooth to unify wireless functionalities:** The Bluetooth Special Interest Group is planning to co-operate more closely with the Wi-Fi, Ultra-wideband (UWB) and Near Field Communications (NFC) wireless standards. The initiative seeks to combine technologies, functionalities and user interfaces to make them more straightforward for end users. Source: http://www.vnunet.com/vnunet/news/2147476/bluetooth-seeks-unify-wireless

- **Enterprise Mobility Spending To Triple By 2008: Study:** According to a report released by the market research firm, Visiongain, spending by enterprises to support wireless and mobile initiatives will almost triple between now and 2008. The study indicated that mobile and wireless spending by enterprises totaled about $50 billion in 2005. That figure will increase to more than $130 billion by the end of 2008. The spending covers hardware, software and services. Source: http://www.mobilepipeline.com/showArticle.jhtml?articleID=175000717.
- **Next-Gen Wi-Fi Could Appear By Late 2006: Study:** According to a study by ABI Research, the pieces are falling into place for the next-generation 802.11n Wi-Fi standard to be ratified and chipsets could appear by the end of 2006. The new standard will provide speeds in excess of Ethernet networking speeds. Source: http://www.mobilepipeline.com/showArticle.jhtml?articleID=175002343.

Wireless Vulnerabilities

- Dell TrueMobile 2300 Remote Authentication Bypass: A vulnerability has been reported which could let a remote malicious user bypass authentication.

[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
December 14, 2005	appfluent.txt	No	Exploit for the Appfluent Technology Database Buffer Overflow vulnerability.
December 14, 2005	Bios.Information.Leakage.txt	N/A	Whitepaper that discusses information leakage and password extraction from a BIOS.
December 14, 2005	fireburn.txt	Yes	Proof of Concept exploit for Firefox 1.0.4 for the InstallVersion.compareTo() vulnerability.
December 14, 2005	lyris_attachment_mssql.pm.txt	Yes	Exploit for the ListManager SQL Injection vulnerability.
December 14, 2005	sugar_suite_40beta.txt	No	Exploit for the SugarCRM Sugar Suite Remote & Local File Include vulnerabilities.
December 13, 2005	mmap_deadlock.c	Yes	Proof of Concept Denial of Service exploit for the Linux

			Kernel Integer Overflow vulnerability.
December 13, 2005	phpcoin_122_incl_xpl.html phpcoin_122_sql_xpl.html	No	Proof of Concept exploit for the PHPCoin File Include vulnerability.
December 13, 2005	phpcoin_122_sql_xpl.html	No	Proof of Concept exploit for the PHPCoin SQL Injection Vulnerability.
December 10, 2005	flatnuke_256_xpl.php flatnuke256_xpl.txt	No	Proof of Concept exploit for the Flatnuke Index.PHP Directory Traversal vulnerability.
December 10, 2005	wiretap.pdf	N/A	A white paper that discusses vulnerabilities and countermeasures that exist within commonly used wiretapping systems by the government.
December 9, 2005	firefox-1.5-buffer-overflow.txt	No	Proof of Concept exploit for the Mozilla History File Remote Denial of Service vulnerability.
December 9, 2005	mambo452_xpl.html	Yes	Exploit for the Mambo Open Source Remote File Include vulnerability.
December 9, 2005	nmap-3.95.tgz	N/A	A utility for port scanning large networks.
December 9, 2005	ttyrpld-2.10.tbz2	N/A	A kernel-based TTY shell, screen, and key logger for Linux, FreeBSD/PCBSD, and OpenBSD that has a real-time log analyzer.
December 8, 2005	openview_connected nodes_exec.pm	Yes	Exploit for the HP OpenView Network Node Manager Remote Arbitrary Code Execution vulnerability.
December 8, 2005	wbaker_260_xpl.php wbaker_260_xpl.txt	No	Proof of Concept exploit for the Website Baker SQL Injection vulnerability.
December 7, 2005	SimpleBBS-cmd-exec.c simplebbs_11_xpl.html bbs.c	No	Proof of Concept exploits for the SimpleBBS Input Validation vulnerability.

[back to top]

Trends

- **Trojan circulates as fake McAfee patch:** A new Trojan is circulating that masquerades as a patch for McAfee's antivirus software. Emails have been spammed out pretending to be a security update for a virus called 'Kongos 31' which does not exist. The email contains a link to a web page hosted in the US that looks very similar to the McAfee download page. Source: http://www.vnunet.com/vnunet/news/2147531/trojan-circulates-fake-mcafee.

- **Cyber Security Tip ST05-019, Preventing and Responding to Identity Theft:** Identity theft, or identity fraud, is a crime that can have substantial financial and emotional consequences. Take precautions with personal information; and if you become a victim, act immediately to minimize the damage. Identity theft, or identity fraud, is a crime that can have substantial financial and emotional consequences. Take precautions with personal information; and if you become a victim, act immediately to minimize the damage. Source: http://www.us-cert.gov/cas/tips/ST05-019.html
- **Cross Domain Vulnerability in Internet Explorer:** US-CERT is aware of a cross domain violation in Internet Explorer. This may allow a script in one domain to access web content in a different domain. Source: http://www.us-cert.gov/current/.
- **New SSL certificates coming:** In an effort to reduce phishing and to help build online trust, security companies and browser makers are working together to design "high assurance" SSL certificates. Source: http://www.securityfocus.com/brief/77.
- **E-Mail Spills Corporate Secrets:** According to a study released by Radicati Group, six percent of workers admitted that they've E-mailed confidential company information to someone they shouldn't have and 62% said they've used their personal accounts for business purposes to circumvent controls placed on their business accounts. Source: http://www.informationweek.com/security/showArticle.jhtml?articleID=174918812.
- **Sober code cracked:** Antivirus companies they have cracked an algorithm that was being used by the Sober worm to "communicate" with its author. The latest variant of the Sober worm caused havoc in November by duping users into executing it by masking itself as e-mails from the FBI and CIA. Source: http://news.com.com/Sober+code+cracked/2100-7349_3-5989094.html?tag=nl.
- **Rootkits Making More Spyware, Adware Stick:** According to F-Secure, the sharp rise in rootkits is due to spyware and adware vendors trying to prevent their wares from being easily uninstalled. Since October the most common rootkit in the wild is the one used by the Apropos spyware program.
  Source: http://www.techweb.com/wire/security/174907374;jsessionid=WRE35TOIAV2AUQSNDBECKH0CJUMEKJVN.
- **Study: Unchecked Software Piracy Could Cost Nations Hundreds of Billions Of Dollars:** According to a study conducted by International Data Corp, without a crackdown on global software piracy, countries stand to lose hundreds of billions of dollars in economic growth and tax revenues and millions of new jobs. Cutting piracy by 10 percent over four years would generate 2.4 million new jobs in information technology, boost economic growth by $400 billion and increase tax revenues worldwide by $67 billion. Source: http://internetweek.cmp.com/security/174907328.

[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	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.
3	Sober-Z	Win32 Worm	Stable	December 2005	A mass-mailing worm that harvests addresses from infected machines, forges the senders email, and utilizes its own mail engine.
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.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.
6	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
7	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.
8	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.
9	Mytob-GH	Win32 Worm	Stable	December 2005	This email worm turns off anti-virus and opens infected systems to remote connections. It further harvests email addresses from infected machines, and forges the senders address.
10	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.

Table updated December 12, 2005

[back to top]

Last updated December 15, 2005