This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing 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.

Bugs, Holes, & Patches

- Windows Operating Systems
  - Brat Designs Breed Remote Denial of Service
  - forumKIT Cross-Site Scripting
  - Gracebyte Network Assistant Remote Denial of Service
  - **Ipswitch IMail Server Remote Buffer Overflow (Updated)**
  - Microsoft Internet Explorer Dynamic IFRAME Security Bypass
  - Microsoft Office RC4 Stream Cipher
  - **Microsoft Windows ANI File Parsing Errors (Updated)**
  - **Microsoft Windows LoadImage API Buffer Overflow (Updated)**
  - **Microsoft Windows HTML Help ActiveX Control (Updated)**
  - **Microsoft Windows Resource Kit 'w3who.dll' Buffer Overflow & Input Validation (Updated)**
  - **Microsoft WINS Name Validation (Updated)**
  - NodeManager SNMPv1 traps Buffer Overflow
  - Multiple Vendors Mozilla/Netscape/Firefox Browser Modal Dialog Spoofing
  - Nullsoft Winamp Multiple Unspecified Vulnerabilities
  - Peer2Mail Password Disclosure
  - RhinoSoft Serv-U FTP Server Remote Denial of Service
  - **VERITAS Backup Exec Buffer Overflow (Updated)**
- UNIX / Linux Operating Systems
  - 4D WebSTAR Grants Access to Remote Users and Elevated Privileges to Local Users
  - **Adobe Acrobat Reader mailListIsPdf() Buffer Overflow (Updated)**
  - **Apache mod_ssl Denial of Service (Updated)**
  - **Apache mod_ssl Remote Denial of Service (Updated)**
  - **Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow (Updated)**
  - **ARJ Software UNARJ Remote Buffer Overflow (Updated)**
  - **Carsten Haitzler imlib Image Decoding Integer Overflow (Updated)**
  - David Mischler Linux IPRoute2 'Netbug' Script Insecure Temporary File
  - Debian Lintian Insecure Temporary File
  - **Ethereal: Multiple security problems (Updated)**
  - FreeRADIUS Server Project Apache 'mod_auth_radius' Integer Overflow
  - **Gallery Cross-Site Scripting (Updated)**
  - Midnight Commander Multiple Vulnerabilities
  - **GNU unrtf process_font_table() Buffer Overflow (Updated)**
  - IohaMail Insecure Default Installation Information Disclosure
  - ImageMagick Photoshop Document Buffer Overflow
  - Jan Kybic BMV Insecure Temporary File Creation
  - **KDE kio_ftp FTP Command Injection Vulnerability (Updated)**
  - **KDE Konqueror Java Sandbox Vulnerabilities (Updated)**
  - **Larry Wall Perl Insecure Temporary File Creation (Updated)**
  - **MIT Kerberos libkadm5srv Heap Overflow (Updated)**
  - MPG123 Layer 2 Frame Header Buffer Overflow
  - **Multiple Vendors Linux Kernel Local RLIMIT_MEMLOCK Bypass Denial of Service (Updated)**
  - **Multiple Vendors Apache mod_dav Remote Denial of Service (Updated)**
  - **Multiple Vendors GNU Exim Buffer Overflows (Updated)**
  - GNU Mailman Multiple Multiple Remote Vulnerabilities
  - **Multiple Vendors Linux Kernel Auxiliary Message Layer State Error (Updated)**
  - **Multiple Vendors Linux Kernel IGMP Integer Underflow (Updated)**
  - **Multiple Vendors Linux Kernel 32bit System Call Emulation and ELF Binary Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Security Modules Escalation Vulnerability (Updated)**
  - **Multiple Vendors nfs-utils 'SIGPIPE' TCP Connection Termination Denial of Service (Updated)**
  - **Multiple Vendors Perl File::Path::rmtree() Permission Modification Vulnerability (Updated)**
  - **Multiple Vendors telnetd-ssl SSL_accept error Format String Flaw (Updated)**

- **Multiple Vendors Linux Kernel EXT3 File System Information Leakage (Updated)**
- **Multiple Vendors LibTIFF TIFFDUMP Heap Corruption Integer Overflow (Updated)**
- Multiple Vendors HylaFAX Remote Access Bypass
- Multiple Vendors Linux Kernel Symmetrical Multiprocessing Page Fault Superuser Privileges
- **Multiple Vendors Linux Kernel Multiple Local MOXA Serial Driver Buffer Overflows (Updated)**
- **Multiple Vendors Linux Kernel AF_UNIX Arbitrary Kernel Memory Modification (Updated)**
- **Multiple Vendors Linux Kernel Random Poolsize SysCTL Handler Integer Overflow (Updated)**
- **Multiple Vendors Linux Kernel uselib() Root Privileges (Updated)**
- Multiple Vendors Linux Kernel Overlapping VMAs
- **Multiple Vendors Linux Kernel BINFMT_ELF Loader Multiple Vulnerabilities (Updated)**
- **Multiple Vendors Linux Kernel SCSI IOCTL Integer Overflow (Updated)**
- **Multiple Vendors Linux Kernel Local DoS & Memory Content Disclosure (Updated)**
- **Multiple Vendors Linux Kernel USB Driver Kernel Memory (Updated)**
- **Multiple Vendors Linux Kernel USB io_edgeport Driver Integer Overflow (Updated)**
- Multiple Vendors 'poppassd_pam' Unauthorized Password Change
- **Namazu Cross-Site Scripting (Updated)**
- **o3read parse_html() Buffer Overflow (Updated)**
- OpenBSD httpd 'mod_include' Buffer Overflow
- OpenBSD TCP Timestamp Remote Denial of Service
- PHPGroupWare 'ACL_Check' Access List Bypass
- PHPWind Administrator Password Modification
- **pizzashack rssh Security Bypass (Updated)**
- **Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities (Updated)**
- SCO UnixWare Mountd Remote Denial of Service
- SGallery Input Validation
- SGI InPerson Superuser Access
- **Squid NTLM fakeauth_auth Helper Remote Denial of Service (Updated)**
- Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow
- SquirrelMail Vacation Plugin 'FTPFile' Input Validation
- Steve Kirkendall Helvis elvprsv Arbitrary File Deletion & Sensitive Information Disclosure
- Solaris Management Console (SMC) Blank Passwords
- **Thibault Godouet Fcron Multiple Vulnerabilities (Updated)**
- **TWiki Search Shell Metacharacter Remote Arbitrary Command Execution (Updated)**
- University of Cambridge Exim 'dns_build_reverse()' Buffer Overflow
- University of Minnesota Gopher Multiple Remote Vulnerabilities
- VideoDB Multiple Vulnerabilities
- Vim Insecure Temporary File Creation

- Multiple Operating Systems
  - Apple ITunes Playlist Buffer Overflow
  - AWStats Multiple Remote Input Validation
  - BiTBOARD Cross-Site Scripting
  - BottomLine Webseries Payment Application Multiple Vulnerabilities
  - SparkleBlog Multiple Input Validation
  - Deutsche Telekom Teledat 530 Remote Denial of Service
  - Dokeos Course Description Cross-Site Scripting
  - Motion MediaPartner Enterprise Multiple Vulnerabilities
  - **GNU TikiWiki Pictures Lets Remote Users Execute Arbitrary Commands (Updated)**
  - Horde 'prefs.php' and 'index.php' Cross-Site Scripting
  - JohnyTech Encrypted Messenger Plug-In Remote Denial of Service
  - Guestserver Input Validation
  - Minis Directory Traversal
  - MPM Guestbook 'top.php' Input Validation
  - Multiple Vendor LDAP Directory Server Buffer Overflow
  - Multiple Vendor Anti-Virus GatewayBase64 Encoded Image Decode Failure
  - **Multiple Vendors Ethereal Multiple Denial of Service & Potential Code Execution Vulnerabilities (Updated)**
  - MySQL MaxDB Remote Buffer Overflow
  - MySQL 'mysqlaccess.sh' Unsafe Temporary Files
  - NETGEAR FVS318 Security Bypass & Cross Site Scripting

- NZEO Zeroboard Multiple Vulnerabilities
- PHP Gift Registry Parameter Input Validation
- **PHP Multiple Remote Vulnerabilities (Updated)**
- Siteman Cross-Site Scripting
- **ViewCVS Ignores 'hide_cvsroot' and 'forbidden' Settings (Updated)**
- WoltLab Burning Board Lite 'addentry.php' Input Validation

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

Bugs, Holes, & Patches

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:

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

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Brat Designs Breed	A remote Denial of Service vulnerability exists when a malicious user submits an empty UDP datagram. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Brat Designs Breed Remote Denial of Service	Low	Securiteam, January 17, 2005
forumKIT forumKIT 1.0	A Cross-Site Scripting vulnerability exists in the 'f.aspx' script due to insufficient sanitization of the 'members' 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 required; however, a Proof of Concept exploit has been published.	forumKIT Cross-Site Scripting	High	SecurityTracker Alert, 1012895, January 14, 2005
Gracebyte Software Gracebyte Network Assistant 3.2.5 .2260	A remote Denial of Service vulnerability exists due to a failure to properly handle UDP datagrams. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Gracebyte Network Assistant Remote Denial of Service	Low	Network Security Team Advisory, January 12, 2005

Ipswitch IMail 8.13	A buffer overflow vulnerability exists in the 'DELETE' command due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code. Patch available at: ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/imail814.exe **Another exploit script has been published.**	Ipswitch IMail Server Remote Buffer Overflow	High	Securiteam, November 15, 2004 SecurityFocus, November 16, 2004 **SecurityFocus, January 11, 2005**
Microsoft Internet Explorer 6.0, SP1&SP2	A vulnerability exists because the security warning can be bypassed when a document contains a specially crafted HTML body tag and a dynamic IFRAME, which could let a remote malicious user bypass the file download security warning mechanism. No workaround or patch available at time of publishing. There is no exploit required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer Dynamic IFRAME Security Bypass	Medium	SecurityFocus, January 15, 2005
Microsoft Office 2000, SR1, SP2&SP3, 2000, SP1, Office XP, SP1-SP3	A security vulnerability exists in the RC4 stream cipher due to incorrect implementation, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Microsoft Office RC4 Stream Cipher	Medium	Bugtraq, January 11, 2005
Microsoft Windows (XP SP2 is not affected)	A Denial of Service vulnerability exists in the parsing of ANI files. A remote user can cause the target user's system to hang or crash. A remote user can create a specially crafted Windows animated cursor file (ANI file) that, when loaded by the target user, will cause the target system to crash. The malicious file can be loaded via HTML, for example. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx **An exploit script has been published.**	Microsoft Windows ANI File Parsing Errors CVE Name: CAN-2004-1305	Low	VENUSTECH Security Lab, December 23, 2004 Microsoft Security Bulletin MS05-002, January 11, 2005 US-CERT Vulnerability Notes, VU#177584 & VU#697136, January 11, 2005 **SecurityFocus, January 12, 2005** **Technical Cyber Security Alert, TA05-012A, January 12, 2005**
Microsoft Windows (XP SP2 is not affected)	An integer overflow vulnerability was reported in the LoadImage API. A remote user can execute arbitrary code. A remote user can create a specially crafted image file that, when processed by the target user, will trigger an overflow in the USER32 library LoadImage API and execute arbitrary code. The code will run with the privileges of the target user. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx A Proof of Concept exploit has been published.	Microsoft Windows LoadImage API Buffer Overflow CVE Names: CAN-2004-1049	High	VENUSTECH Security Lab. December 23, 2004 Microsoft Security Bulletin MS05-002, January 11, 2005 US-CERT Vulnerability Note, VU#625856, January 11, 2005 **Technical Cyber Security Alert, TA05-012A, January 12, 2005**

Microsoft Windows 2000 SP3 & SP4, XP SP1 & SP2, XP 64-Bit Edition SP1, XP 64-Bit Edition Version 2003, Windows Server 2003, Windows Server 2003 64-Bit Edition, Windows 98, 98SE, ME	A cross-domain vulnerability exists in the HTML Help ActiveX control, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS05-001.mspx Exploits have been published.	Microsoft Windows HTML Help ActiveX Control CVE Name: CAN-2004-1043	High	Microsoft Security Bulletin MS05-001, January 11, 2005 **Technical Cyber Security Alert ,TA05-012B, January 12, 2005** **US-CERT Vulnerability Note, VU#972415, January 18, 2005**
Microsoft Windows 2000/XP Resource Kit	Several vulnerabilities exist in the 'w3who.dll' Microsoft ISAPI extension in the Windows 2000/XP Resource Kit: Cross-Site Scripting vulnerabilities exist when displaying HTTP headers and in error messages, which could let a remote malicious user execute arbitrary HTML and script code; and a buffer overflow vulnerability exists when processing input parameters, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. **An exploit script has been published.**	Microsoft Windows Resource Kit 'w3who.dll' Buffer Overflow & Input Validation CVE Names: CAN-2004-1133 CAN-2004-1134	High	Exaprobe Security Advisory, December 6, 2004 **SecurityFocus, January 11, 2005**
Microsoft Windows NT Server 4.0 SP 6a, NT Server 4.0 Terminal Server Edition SP 6, Windows 2000 Server SP 3 & SP4, Windows Server 2003, 2003 64-Bit Edition	A vulnerability exists due to an unchecked buffer in the handling of the 'Name' parameter from certain packets, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-045.mspx **An exploit script has been published.**	Microsoft WINS Name Validation CVE Name: CAN-2004-0567	High	Microsoft Security Bulletin, SB04-045, December 14, 2004 US-CERT Vulnerability Note, VU#378160, December 16, 2004 Packetstorm, January 2, 2005 **SecurityFocus, January 11, 2005**
Mnet Soft Factor NodeManager Professional version 2.00	A buffer overflow vulnerability exists due to a boundary error when logging SNMPv1 traps, which could let a remote malicious user execute arbitrary code. Update available at: http://www.h4.dion.ne.jp/~you4707/NodeManagerPro.html Currently we are not aware of any exploits for this vulnerability.	NodeManager SNMPv1 Traps Buffer Overflow	High	Securiteam, January 18, 2005
Multiple Vendors Mozilla Browser 1.7.5, Firefox 1.0, Netscape Netscape 7.1	A vulnerability exists because popup windows can overlay modal dialogs, which could lead to a false sense of security. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Mozilla/Netscape/Firefox Browser Modal Dialog Spoofing	Medium	Securiteam, January 11, 2005
Nullsoft Winamp 5.0 1-5.0 8	Vulnerabilities exist in 'in_mp4.dll,' 'enc_mp4.dll,' 'libmp4v2.dll' and a buffer overflow vulnerability exists in 'in_cdda.dll'. The impact was not specified. Upgrades available at: http://forums.winamp.com/showthread.php?s=&threadid=202799 Currently we are not aware of any exploits for these vulnerabilities.	Nullsoft Winamp Multiple Unspecified Vulnerabilities	Not Specified	SecurityTracker Alert, 1012880, January 14, 2005
peer2mail.com peer2mail 1.4 & prior	A vulnerability exists in the 'p2m.exe' process, which could let a malicious user obtain the password from memory. No workaround or patch available at time of publishing.	Peer2Mail Password Disclosure	Medium	SecurityTracker Alert, 1012912, January 16, 2005

	Currently we are not aware of any exploits for this vulnerability.			
RhinoSoft Serv-U 2.5	A remote Denial of Service vulnerability exists because multiple connection attempts are not handled properly. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	RhinoSoft Serv-U FTP Server Remote Denial of Service	Low	SecurityFocus, January 10, 2005
Veritas Software Backup Exec 8.0, 8.5, 8.6, 9.0, 9.1	A buffer overflow vulnerability exists due to a boundary error in the Agent Browser service when processing received registration requests, which could let a remote malicious user execute arbitrary code. Hotfix available at: http://seer.support.veritas.com/docs/273422.htm **Exploit scripts have been published.**	VERITAS Backup Exec Buffer Overflow CVE Name: CAN-2004-1172	High	Veritas Software Security Advisory, 273419, December 16, 2004 **SecurityFocus, January 11, 2005** **US-CERT Vulnerability Note, VU#907729, January 15, 2005**

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	
4D, Inc. 4D WebSTAR 5.3.2 and prior versions	Multiple vulnerabilities exist including a buffer overflow that could allow a malicious user to escalate privileges or obtain access to protected resources. A remote user can issue a specially crafted FTP command to trigger a stack-based overflow and execute arbitrary code. The vendor has released a fixed version (5.3.3), available at: http://www.4d.com/products/downloads_4dws.html **An exploit script has been published.**	4D WebSTAR Grants Access to Remote Users and Elevated Privileges to Local Users	High	SecurityT 1010696, **SecurityF 11, 2005**
Adobe Adobe Acrobat Reader 5.0.9 for Unix	A buffer overflow vulnerability exists in in Adobe Acrobat Reader for Unix. A remote malicious user can execute arbitrary code on the target system. A remote user can create a specially crafted PDF file that, when processed by the target user, will trigger a buffer overflow in the mailListIsPdf() function and execute arbitrary code. The code will run with the privileges of the target user. The vendor has issued a fixed version (5.0.10): http://www.adobe.com/support/techdocs/331153.html Gentoo: http://www.gentoo.org/security/en/glsa/ glsa-200412-12.xml Red Hat: http://rhn.redhat.com/errata/RHSA-2004-674.html **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Adobe Acrobat Reader mailListIsPdf() Buffer Overflow CVE Name: CAN-2004-1152	High	iDEFENS Advisory Gentoo S GLSA 200 acroread, 2004 Red Hat: RHSA-20 Decembe **SUSE Se Report, SUSE-SR January**
Apache Software Foundation Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.50	A remote Denial of Service vulnerability exists in Apache 2 mod_ssl during SSL connections. Apache: http://nagoya.apache.org/bugzilla/ show bug.cgi?id=29964 RedHat: http://rhn.redhat.com/errata/RHSA-2004-349.html SUSE: ftp://ftp.SUSE.com/pub/SUSE/i386/update/	Apache mod_ssl Denial of Service CVE Name: CAN-2004-0748	Low	SecurityF 6, 2004 Mandrake Update A MDKSA-2 Septembe Gentoo Li Advisory, Septembe Trustix Se

	Gentoo: http://security.gentoo.org/glsa/glsa-200409-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/ HP: http://software.hp.com Apple: http://www.apple.com/swupdates/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub** **/TurboLinux/TurboLinux/** Currently we are not aware of any exploits for this vulnerability.			Security Advisory, Septembe Conectiva Announce CLA-2004 23, 2004 Fedora U FEDORA- Septembe HP Secur HPSBUX 26, 2004 Apple Sec APPLE-S Decembe **TurboLin** **Announc** **TLSA-20** **13, 2005**
Apache Software Foundation Apache 2.0.50	A remote Denial of Service vulnerability exists in 'char_buffer_read()' when using a RewriteRule to reverse proxy SSL connections. Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126 SUSE: ftp://ftp.SUSE.com/pub/SUSE/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/ RHSA-2004-463.html Gentoo: http://security.gentoo.org/glsa/ glsa-200409-21.xml Trustix: http://www.trustix.org/errata/2004/0047/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/ HP: http://h30097.www3.hp.com/internet/ download.htm Apple: http://www.apple.com/swupdates/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/** **TurboLinux/TurboLinux/** There is no exploit code required; however, Proofs of Concept exploits have been published.	Apache mod_ssl Remote Denial of Service CVE Name: CAN-2004-0751	Low	SecurityT 1011213, 2004 Mandrake Update A MDKSA-2 Septembe RedHat S RHSA-20 Septembe Gentoo Li Advisory Septembe Trustix Se Security A TSLSA-20 Septembe Conectiva Announce CLA-2004 23, 2004 Fedora U FEDORA- Septembe HP Secur HPSBUX HPSBGN & 29, 200 Apple Sec APPLE-S Decembe **TurboLin** **Announc** **TLSA-20** **13, 2005**

Apache Software Foundation Gentoo Mandrake OpenBSD OpenPKG RedHat SGI Tinysofa Trustix Apache 1.3-2.0.49	A stack-based buffer overflow has been reported in the Apache mod_ssl module. This issue would most likely result in a Denial of Service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures. Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&r2=1.106 Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org Tinysofa: http://www.tinysofa.org/support/errata/2004/008.html Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200406-05.xml OpenBSD: http://www.openbsd.org/errata.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/ Apple: http://www.apple.com/support/security/security_updates.html Fedora Legacy: http://download.fedoralegacy.org/redhat/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** Currently we are not aware of any exploits for this vulnerability.	Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow CVE Name: CAN-2004-0488	Low/High (High if arbitrary code can be executed)	Security F 2004 Gentoo Li Advisory, June 9, 2 Mandrake Update A MDKSA-2 June 1. 2 OpenPKG Advisory, OpenPKG May 27, 2 RedHat S RHSA-20 2004 SGI Secu 20040605 2004 Tinysofa TSSA-200 2004 Trustix Se TSLSA-20 2004 Fedora Le Advisory, October 1 **TurboLin** **Announc** **TLSA-20** **13, 2005**
ARJ Software Inc. UNARJ 2.62-2.65	A buffer overflow vulnerability exists due to insufficient bounds checking on user-supplied strings prior to processing, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-29.xml SUSE: http://www.suse.de/de/security/2004_03_sr.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-007.html** Currently we are not aware of any exploits for this vulnerability.	ARJ Software UNARJ Remote Buffer Overflow CVE Name: CAN-2004-0947	High	SecurityT 1012194, 2004 Gentoo Li Advisory, Novembe SUSE Se Report SU Decembe Fedora U FEDORA- Decembe **RedHat S** **RHSA-20** **January**
Carsten Haitzler imlib 1.x	Multiple vulnerabilities exist due to integer overflows within the image decoding routines. This can be exploited to cause buffer overflows by tricking a user into viewing a specially crafted image in an application linked against the vulnerable library. Gentoo: http://security.gentoo.org/glsa/glsa-200412-03.xml	Carsten Haitzler imlib Image Decoding Integer Overflow CVE Name: CAN-2004-1026 CAN-2004-1025	High	Secunia A SA13381, 2004 Red Hat A RHSA-20 Decembe

	Red Hat: http://rhn.redhat.com/errata/RHSA-2004-651.html SUSE: http://www.suse.com/en/private/download/updates Debian: http://www.debian.org/security/2004/dsa-618 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imlib2/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities.			SecurityF 14, 2004 Debian D Decembe **Mandrak** **Update A** **MDKSA-2** **12, 2005**
David Mischler IPRoute 20010824, 0.973, 0.974, 1.10, 1.18, 2.2.4, 2.4.7,	A vulnerability exists in the 'netbug' script because temporary files are created in an insecure manner, which could let a malicious user delete arbitrary files. No workaround or patch available at time of publishing. There is no exploit required	David Mischler Linux IPRoute2 'Netbug' Script Insecure Temporary File	Medium	Secunia A SA13758,
Debian lintian 1.2 0.17.1	A vulnerability exists because temporary files are created in an insecure manner, which could let a malicious user delete arbitrary files. Upgrade available at: http://security.debian.org/pool/updates/ main/l/lintian/lintian_1.20.17.1_all.deb There is no exploit required.	Debian Lintian Insecure Temporary File CVE Name: CAN-2004-1000	Medium	Debian Se DSA, 630 2004
Ethereal Ethereal 0.x	Multiple Denial of Service and buffer overflow vulnerabilities exist due to errors in the iSNS, SNMP, and SMB dissectors which may allow an attacker to run arbitrary code or crash the program. Updates available at: http://www.ethereal.com/download.html or disable the affected protocol dissectors. Fedora: http://download.fedora.redhat.com/pub/fedora/ linux/core/updates/1/ Debian: http://lists.debian.org/debian-security- announce/debian- security-announce -2004/msg00129.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** An exploit script has been published.	Ethereal: Multiple security problems CVE Names: CAN-2004-0633 CAN-2004-0634 CAN-2004-0635	Low/High (High if arbitrary code can be executed)	Gentoo Li Advisory, Ethereal, Secunia A 12035, Ju Ethereal A enpa-sa-0 US-CERT Notes VU VU#8294 Septembe **Conectiv** **Announc** **CLA-2005** **2005**
FreeRADIUS Server Project mod_auth_radius 1.3.9, 1.5, 1.5.2, 1.5.4	A vulnerability exists in the 'radcpy()' function in the 'mod_auth_radius' module for Apache when handling server-supplied integer values, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	FreeRADIUS Server Project Apache 'mod_auth_radius' Integer Overflow	Low/High (High if arbitrary code can be executed)	LSS Secu LSS-2005 10, 2005
Gallery Project Gallery 1.4 -pl1&pl2, 1.4, 1.4.1, 1.4.2, 1.4.3 -pl1 & pl2; Gentoo Linux	A Cross-Site Scripting vulnerability exists in several files, including 'view_photo.php,' 'index.php,' and 'init.php' due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://sourceforge.net/project/showfiles. php?group_id=7130 Gentoo: http://security.gentoo.org/glsa/glsa-200411-10.xml **Debian:**	Gallery Cross-Site Scripting	High	Gentoo Li Advisory, 200411-1 2004 **Debian S** **DSA 642-** **2005**

	http://security.debian.org/pool/updates/main/g/gallery/ There is no exploit code required.			
GNU Midnight Commander Project Midnight Commander 4.x	Multiple vulnerabilities exist due to various design and boundary condition errors, which could let a remote malicious user cause a Denial of Service, obtain elevated privileges, or execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/m/mc/ Currently we are not aware of any exploits for these vulnerabilities.	Midnight Commander Multiple Vulnerabilities CVE Names: CAN-2004-1004 CAN-2004-1005 CAN-2004-1009 CAN-2004-1090 CAN-2004-1091 CAN-2004-1092 CAN-2004-1093 CAN-2004-1174 CAN-2004-1175 CAN-2004-1176	Low/ Medium/ High (Low if a DoS; Medium is elevated privileges can be obtained; and High if arbitrary code can be executed)	SecurityT 1012903,
GNU unrtf 0.19.3	A vulnerability was reported in unrtf. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted RTF file that, when processed by the target user with unrtf, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the process_font_table() function in 'convert.c.'. **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200501-15.xml** A Proof of Concept exploit script has been published.	GNU unrtf process_font_table() Buffer Overflow	High	SecurityT 1012595, 2004 **Gentoo L Advisory 200501-1 2005**
ilohamail.org IohaMail 0.8.6-0.8.13, 0.8.14 RC1&RC2	A vulnerability exists in the default installation due to a failure to securely install sensitive files, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit required.	IohaMail Insecure Default Installation Information Disclosure	Medium	Secunia A SA13807,
ImageMagick ImageMagick 6.x	A buffer overflow vulnerability exists in 'coders/psd.c' when a specially crafted Photoshop document file is submitted, which could let a remote malicious user execute arbitrary code. Update available at: http://www.imagemagick.org/www/download.html Currently we are not aware of any exploits for this vulnerability.	ImageMagick Photoshop Document Buffer Overflow	High	iDEFENS Advisory,
Jan Kybic BMV 1.2	A vulnerability exists in 'gsinterf.c' due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/b/bmv/bmv_1.2-14.2_i386.deb There is no exploit required.	BMV Insecure Temporary File Creation CVE Name: CAN-2003-0014	Medium	Debian S DSA 633- 2005
KDE KDE 3.x, 2.x	A vulnerability exists in kio_ftp, which can be exploited by malicious people to conduct FTP command injection attacks. The vulnerability has been fixed in the CVS repository. Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:160 Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-18.xml**	KDE kio_ftp FTP Command Injection Vulnerability CVE Name: CAN-2004-1165	Medium	KDE Advi Decembe Debian S DSA 631- 2005 **Gentoo L Advisory 200501-1 2005**

	Currently we are not aware of any exploits for this vulnerability.			
KDE Konqueror prior to 3.32	Two vulnerabilities exist in KDE Konqueror, which can be exploited by malicious people to compromise a user's system.The vulnerabilities are caused due to some errors in the restriction of certain Java classes accessible via applets and Javascript. This can be exploited by a malicious applet to bypass the sandbox restriction and read or write arbitrary files. Update to version 3.3.2: http://kde.org/download/ Apply patch for 3.2.3: ftp://ftp.kde.org/pub/kde/security_patches/post-3.2.3-kdelibs-khtml-java.tar.bz2 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:154 **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-16.xml** Currently we are not aware of any exploits for these vulnerabilities.	KDE Konqueror Java Sandbox Vulnerabilities CVE Name: CAN-2004-1145	High	KDE Secu Decembe Mandrake MDKSA-2 Decembe US-CERT Note, VU# 5, 2005 **Gentoo L** **Advisory** **200501-1** **2005**
Larry Wall Perl 5.8.3	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200412-04.xml Debian: http://security.debian.org/pool/updates/main/p/perl/ **OpenPKG:** **ftp://ftp.openpkg.org/release/2.1/UPD/perl-5.8.4-2.1.1.src.rpm** There is no exploit code required.	Perl Insecure Temporary File Creation CVE Name: CAN-2004-0976	Medium	Trustix Se Advisory, Septembe Ubuntu S USN-16-1 2004 Gentoo Li Advisory, Decembe Debian S DSA 620- 2004 **OpenPK** **Advisory** **OpenPK** **January**
MIT Kerberos 5 krb5-1.3.5 and prior	A buffer overflow exists in the libkadm5srv administration library. A remote malicious user may be able to execute arbitrary code on an affected Key Distribution Center (KDC) host. There is a heap overflow in the password history handling code. A patch is available at: http://web.mit.edu/kerberos/advisories/2004-004-patch_1.3.5.txt Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-05.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/k/krb5/** Currently we are not aware of any exploits for this vulnerability.	Kerberos libkadm5srv Heap Overflow CVE Name: CAN-2004-1189	High	SecurityT 1012640, 2004 Gentoo G January 5 **Ubuntu S** **USN-58-1** **2005** **Conectiv** **Announc** **CLA-2005** **2005**
mpg123 mpg123 0.59 m-0.59 s	A buffer overflow vulnerability exists when parsing frame headers for layer-2 streams, which could let a remote malicious user execute arbitrary code. Gentoo:	MPG123 Layer 2 Frame Header Buffer Overflow	High	Gentoo Li Advisory, January 1

	http://security.gentoo.org/glsa/glsa-200501-14.xml Currently we are not aware of any exploits for this vulnerability.	CVE Name: CAN-2004-0991		
Multiple Vendors Linux kernel 2.6.10, 2.6.9; **RedHat Fedora Core2&3**	A Denial of Service vulnerability exists in the 'mlockall()' system call due to a failure to properly enforce defined limits. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** A Proof of Concept exploit script has been published.	Linux Kernel Local RLIMIT_MEMLOCK Bypass Denial of Service	Low	Bugtraq, J **Fedora U Notificati FEDORA January**
Multiple Vendors Apache Software Foundation Apache 2.0.50 & prior; Gentoo Linux 1.4; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A remote Denial of Service vulnerability exists in the Apache mod_dav module when an authorized malicious user submits a specific sequence of LOCK requests. Update available at: http://httpd.apache.org/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml RedHat: ftp://updates.redhat.com/enterprise Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/liba/ HP: http://software.hp.com IBM: http://www-1.ibm.com/support/docview.wss?uid=swg21190212 **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** There is no exploit code required; however, a Proof of Concept exploit has been published.	Apache mod_dav Remote Denial of Service CVE Name: CAN-2004-0809	Low	SecurityT 1011248, 2004 Conectiva Announce CLA-2004 23, 2004 Fedora U FEDORA- Septembe Debian S DSA 558- 2004 HP Secur HPSBUX 26, 2004 1190212 IBM Grou 1190212, 2004 **TurboLin Announc TLSA-20 13, 2005**

Multiple Vendors Exim 4.43 & prior	Multiple vulnerabilities exist that could allow a local user to obtain elevated privileges. There are buffer overflows in the host_aton() function and the spa_base64_to_bits() functions. It may be possible to execute arbitrary code with the privileges of the Exim process. The vendor has issued a fix in the latest snapshot: ftp://ftp.csx.cam.ac.uk/pub/software /email/exim/ Testing/exim-snapshot.tar.gz ftp://ftp.csx.cam.ac.uk/pub/software/ email/exim/Testing/exim-snapshot.tar.gz.sig Also, patches for 4.43 are available at: http://www.exim.org/mail-archives/ exim-announce/2005/msg00000.html Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/e/exim4/ Gentoo: http://security.gentoo.org/glsa/ glsa-200501-23.xml **Debian:** **http://security.debian.org/pool/** **updates/main/e/exim/** Currently we are not aware of any exploits for these vulnerabilities.	GNU Exim Buffer Overflows CVE Names: CAN-2005-0021 CAN-2005-0022	High	SecurityT 1012771, Gentoo Li Advisory, January 1 **Debian S** **DSA 635-** **January**
Multiple Vendors GNU Mailman 1.0, 1.1, 2.0 beta1-beta3, 2.0-2.0 .3, 2.0.5-2.0 .8, 2.0.1-2.0.14, 2.1 b1, 2.1- 2.1.5; Ubuntu Linux 4.1, ia64, ia32	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists when returning error pages due to insufficient sanitization by 'scripts/driver,' which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists due to a weakness in the automatic password generation algorithm, which could let a remote malicious user brute force automatically generated passwords. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ m/mailman/ Currently we are not aware of any exploits for these vulnerabilities.	GNU Mailman Multiple Multiple Remote Vulnerabilities CVE Names: CAN-2004-1143 CAN-2004-1177	Medium/ High (High if arbitrary code can be executed)	SecurityT 12, 2005
Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9; **Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0**	A vulnerability was reported in the Linux kernel in the auxiliary message (scm) layer. A local malicious user can cause Denial of Service conditions. A local user can send a specially crafted auxiliary message to a socket to trigger a deadlock condition in the __scm_send() function. Ubuntu: http://security.ubuntu.com/ubuntu/pool/ SUSE: http://www.novell.com/linux/security/ advisories/2004_44_kernel.html Trustix: http://http.trustix.org/pub/trustix/updates/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-689.html Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ **Avaya:** **http://support.avaya.com/elmodocs2/** **security/ASA-2005-006_RHSA-2004-549** **RHSA-2004-505RHSA-2004-689.pdf** A Proof of Concept exploit script has been published.	Multiple Vendors Linux Kernel Auxiliary Message Layer State Error CVE Name: CAN-2004-1016	Low	iSEC Sec Advisory 14, 2004 SecurityF 25, 2004 Secunia, 4, 2005 **Avaya Se** **ASA-200** **14, 2006**

Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9; **Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0**	Several vulnerabilities exist in the Linux kernel in the processing of IGMP messages. A local user may be able to gain elevated privileges. A remote user can cause the target system to crash. These are due to flaws in the ip_mc_source() and igmp_marksources() functions. SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf** A Proof of Concept exploit script has been published.	Multiple Vendors Linux Kernel IGMP Integer Underflow CVE Name: CAN-2004-1137	Low/ Medium (Medium if elevated privileges can be obtained)	iSEC Sec Advisory 14, 2004 SecurityF 25, 2005 Secunia, 4, 2005 **Avaya Se ASA-2005 14, 2006**
Multiple Vendors Linux Kernel 2.4.x; **Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0**, **Network Routing**	Two vulnerabilities exist in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or potentially gain escalated privileges. 1) A boundary error exists in the system call handling in the 32bit system call emulation on AMD64 / Intel EM64T systems. 2) An unspecified error within the memory management handling of ELF executables in "load_elf_binary" can be exploited to crash the system via a specially crafted ELF binary (this issue only affects Kernel versions prior to 2.4.26). Issue 2 has been fixed in Kernel version 2.4.26 and later. Red Hat: http://rhn.redhat.com/errata/RHSA-2004-689.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel 32bit System Call Emulation and ELF Binary Vulnerabilities CVE Name: CAN-2004-1144 CAN-2004-1234	Medium	Secunia, Decembe Red Hat F Decembe **Avaya Se ASA-2005 14, 2006**
Multiple Vendors Linux Security Modules (LSM); **Ubuntu Linux 4.1 ppc, ia64, ia32**	A security issue in Linux Security Modules (LSM) may grant normal user processes escalated privileges. When loading the Capability LSM module as a loadable kernel module, all existing processes gain unintended capabilities granting them root privileges. Only use the Capability LSM module when compiled into the kernel and grant only trusted users access to affected systems. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Security Modules Escalation Vulnerability **CVE Name:** **CAN-2004-1337**	High	Secunia S Decembe **Ubuntu S USN-57-1**
Multiple Vendors nfs-utils 1.0.6	A vulnerability exists due to an error in the NFS statd server in 'statd.c' where the 'SIGPIPE' signal is not correctly ignored. This can be exploited to crash a vulnerable service via a malicious peer terminating a TCP connection prematurely. Upgrade to 1.0.7-pre1: http://sourceforge.net/project/showfiles.php?group_id=14&package_id=174 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:146 Debian: http://www.debian.org/security/2004/dsa-606 Red Hat:	Multiple Vendors nfs-utils 'SIGPIPE' TCP Connection Termination Denial of Service CVE Name: CAN-2004-0946 CAN-2004-1014	Low	Secunia A SA13384, 2004 Debian S DSA-606- Decembe Red Hat S RHSA-20 Decembe **Mandrak Update A MDKSA-2 12, 2005**

	http://rhn.redhat.com/errata/RHSA-2004-583.html **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Perl	A race condition vulnerability was reported in the 'File::Path::rmtree()' function. A remote user may be able to obtain potentially sensitive information. A remote user may be able to obtain potentially sensitive information or modify files. The vendor has released Perl version 5.8.4-5 to address this vulnerability. Customers are advised to contact the vendor for information regarding update availability. Debian: http://security.debian.org/pool/updates/main/p/perl/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/perl/ **OpenPKG:** **ftp://ftp.openpkg.org/release/2.1/UPD/** **perl-5.8.4-2.1.1.src.rpm** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Perl File::Path::rmtree() Permission Modification Vulnerability CVE Name: CAN-2004-0452	Medium	Ubuntu S USN-44-1 2004 Debian S DSA 620- 2004 **OpenPK Advisory OpenPK January**
Multiple Vendors telnetd-ssl	A format string vulnerability exists that could allow a remote user to cause arbitrary code to be executed on the target system. The flaw resides in 'telnetd/telnetd.c' in the processing of SSL error messages. Debian: http://www.debian.org/security/2004/dsa-616 Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors telnetd-ssl SSL_accept error Format String Flaw CVE Name: CAN-2004-0998	High	SecurityT 1012666, 2004 **US-Cert V Note, VU 14, 2005**
Multiple Vendors Unix Linux kernel 2.4, 2.4 .0-test1 test12, 2.4.1 2.4.25, 2.6, test1 test11, 2.6.1 -rc1&rc2, 2.6.2 2.6.4; **Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0**	A vulnerability exists in the Linux kernel when writing to an ext3 file system due to a design error that causes some kernel information to be leaked, which could let a malicious user obtain sensitive information. Upgrade available at: http://www.kernel.org/pub/linux /kernel/v2.4/linux-2.4.26.tar.bz2 Conectiva: ftp://ul.conectiva.com.br/updates/1.0/ Debian: http://security.debian.org/pool/updates/main/k/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat (updated kernel package): http://rhn.redhat.com/errata/ RHSA-2004-504.html Trustix: http://http.trustix.org/pub/trustix/updates/ Engarde: http://infocenter.guardiandigital.com/advisories/ **Avaya:** **http://support.avaya.com/elmodocs2/** **security/ASA-2005-006_RHSA-2004-549** **RHSA-2004-505RHSA-2004-689.pdf** We are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel EXT3 File System Information Leakage CVE Name: CAN-2004-0177	Medium	Mandrake Update A MDKSA-2 2004 Trustix Se Security A TSLSA-20 2004 Debian S DSA 489- 17, 2004 Conectiva Advisory, April 15, 2 Red Hat S Advisories RHSA-20 166-08, A Guardian Advisory, ESA-2004 28, 2004 Red Hat S Advisories RHSA-20 505-13, D **Avaya Se ASA-2005 14, 2006**
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc,	A vulnerability exists in the tiffdump utility, which could let a remote malicious user execute arbitrary code. Debian:	LibTIFF TIFFDUMP Heap Corruption Integer Overflow	High	SecurityT 1012785, **RedHat S**

mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux; LibTIFF LibTIFF 3.4, 3.5.1-3.5.5, 3.5.7, 3.6 .0, 3.6.1, 3.7, 3.7.1; RedHat Fedora Core2& Core 3; Ubuntu Ubuntu Linux 4.1 ppc, ia64, ia32	http://security.debian.org/pool/updates/main/t/tiff/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/t/tiff/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-019.html** Currently we are not aware of any exploits for this vulnerability.	CVE Name: CAN-2004-1183		**RHSA-20** **January**
Multiple Vendors Hylafax.org Hylafax 4.0 pl0-pl2, 4.0.2, 4.1, beta1-beta3, 4.1.1-4.1.3, 4.1.5-4.1.8; 4.2; MandrakeSoft Linux Mandrake 10.0, AMD64, 10.1 X86_64, 10.1	A vulnerability exists because the username is incorrectly compared with an entry in the 'hosts.hfaxd' database, which could let a remote malicious user obtain unauthorized access. Patches available at: ftp://ftp.hylafax.org/source/hylafax-4.2.1.tar.gz Debian: http://security.debian.org/pool/updates/main/h/hylafax/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php There is no exploit required.	HylaFAX Remote Access Bypass CVE Name: CAN-2004-1182	Medium	SecurityT 101284, J
Multiple Vendors Linux kernel 2.2-2.2.27 -rc1, 2.4-2.4.29 -rc1, 2.6 .10, 2.6-2.6.10	A race condition vulnerability exists in the page fault handler of the Linux Kernel on symmetric multiprocessor (SMP) computers, which could let a malicious user obtain superuser privileges. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Exploit scripts have been published.	Linux Kernel Symmetrical Multiprocessing Page Fault Superuser Privileges CVE Name: CAN-2005-0001	High	SecurityT 1012862,
Multiple Vendors Linux kernel 2.2-2.2.25, 2.3, 2.3.99, pre1-pre7, 2.4 .0, test1-test12, 2.4-2.4.28, 2.4.29 -rc2, 2.5 .0-2.5.65	Multiple buffer overflow vulnerabilities exist in the 'drivers/char/moxa.c' file due to insufficient bounds checks prior to copying user-supplied data to fixed-size memory buffers, which could let a malicious user execute arbitrary code. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Local MOXA Serial Driver Buffer Overflows	High	Bugtraq, **Ubuntu S** **USN-60-0** **2005**

Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.27; **Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0**	A vulnerability exists in the 'AF_UNIX' address family due to a serialization error, which could let a malicious user obtain elevated privileges or possibly execute arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Red Hat: http://rhn.redhat.com/errata/RHSA-2004-504.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel AF_UNIX Arbitrary Kernel Memory Modification CVE Name: CAN-2004-1068	Medium/ High (High if arbitrary code can be executed)	Bugtraq, I 2004 SUSE Se Report, SUSE-SR Decembe SecurityF 14, 2004 Fedora U Notificatio FEDORA- January 4 **Avaya Se ASA-2005 14, 2006**
Multiple Vendors Linux kernel 2.4, 2.4 .0 test1-test 12, 2.4-2.4.28, 2.4.29 -rc2, 2.6 .10, 2.6, test1-test11, 2.6.1-2.6.10, 2.6.10 rc; **RedHat Fedora Core2&3**	An integer overflow vulnerability exists in the 'random.c' kernel driver due to insufficient sanitization of the 'poolsize_strategy' function, which could let a malicious user cause a Denial of Service or execute arbitrary code. **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** A Proof of Concept exploit script has been published.	Linux Kernel Random Poolsize SysCTL Handler Integer Overflow	Low/High (High if arbitrary code can be executed)	Bugtraq, J **Fedora U Notificati FEDORA January**
Multiple Vendors Linux Kernel 2.4.0 test1-test12, 2.4-2.4.28, 2.4.29 -rc2, 2.6, test1-test11, 2.6.1, rc1-rc2, 2.6.2-2.6.9, 2.6.10 rc2	A vulnerability exists in the 'load_elf_library()' function in 'binfmt_elf.c' because memory segments are properly processed, which could let a remote malicious user execute arbitrary code with root privileges. **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Trustix: http://http.trustix.org/pub/trustix/updates/** A Proof of Concept exploit script has been published.	Linux Kernel uselib() Root Privileges CVE Name: CAN-2004-1235	High	iSEC Sec Advisory, **Fedora U Notificati FEDORA January** **Trustix S Security TSLSA-2 January**
Multiple Vendors Linux kernel 2.4.0-test1-test12, 2.4-2.4.28, 2.4.29 -rc1&rc2	A vulnerability exists in the processing of ELF binaries on IA64 systems due to improper checking of overlapping virtual memory address allocations, which could let a malicious user cause a Denial of Service or potentially obtain root privileges. Patch available at: http://linux.bkbits.net:8080/linux-2.6/cset@41a6721cce-LoPqkzKXudYby_3TUmg Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Overlapping VMAs CVE Name: CAN-2005-0003	Low/High (High if root access can be obtained)	Trustix Se Security A TSLSA-20 13, 2005

Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.8 SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9; **Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0**	Multiple vulnerabilities exist due to various errors in the 'load_elf_binary' function of the 'binfmt_elf.c' file, which could let a malicious user obtain elevated privileges and potentially execute arbitrary code. Patch available at: http://linux.bkbits.net:8080/linux-2.6/gnupatch@41925edcVccsXZXObG444GFvEJ94GQ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html Red Hat: http://rhn.redhat.com/errata/RHSA-2004-549.html RedHat: http://rhn.redhat.com/errata/RHSA-2004-504.html http://rhn.redhat.com/errata/RHSA-2004-505.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf** Proofs of Concept exploit scripts have been published.	Multiple Vendors Linux Kernel BINFMT_ELF Loader Multiple Vulnerabilities CVE Names: CAN-2004-1070 CAN-2004-1071 CAN-2004-1072 CAN-2004-1073	Medium/ High (High if arbitrary code can be executed)	Bugtraq, I 2004 Fedora U Notificatio FEDORA- Novembe SUSE Se Report, SUSE-SA Decembe Red Hat A RHSA-20 Decembe RedHat S RHSA-20 505-14, D **Avaya Se ASA-2005 14, 2006**
Multiple Vendors Linux Kernel 2.6 .10, 2.6, test-test11, 2.6.1-2.6.10, 2.6.10 rc2; **RedHat Fedora Core2&3**	An integer overflow vulnerability exists in the 'scsi_ioctl.c' kernel driver due to insufficient sanitization of the 'sg_scsi_ioctl' function, which could let a malicious user execute arbitrary code. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SCSI IOCTL Integer Overflow	High	Bugtraq, J **Fedora U Notificati FEDORA January**
Multiple Vendors Linux kernel 2.6.x, 2.4.x , SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9; Turbolinux Turbolinux Server 10.0	Two vulnerabilities exist: a Denial of Service vulnerability exists via a specially crafted 'a.out' binary; and a vulnerability exists due to a race condition in the memory management, which could let a malicious user obtain sensitive information. SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/RPMS/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel Local DoS & Memory Content Disclosure CVE Name: CAN-2004-1074	Low/ Medium (Medium if sensitive information can be obtained)	Secunia A SA13308, 2004 SUSE Se Report, SUSE-SA Decembe SecurityF 16, 2004 **Trustix S Security TSLSA-2 January**
Multiple Vendors Linux Kernel USB Driver prior to 2.4.27; **Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular**	A vulnerability exists in certain USB drivers because uninitialized structures are used and then 'copy_to_user(...)' kernel calls are made from these structures, which could let a malicious user obtain obtain uninitialized kernel memory contents. Update available at: http://kernel.org/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200408-24.xml	Multiple Vendors Linux Kernel USB Driver Kernel Memory CVE Name: CAN-2004-0685	Medium	US-CERT VU#9811 2004 Trustix, T kernel, Au Red Hat S Advisorie RHSA-20 505-13, D

Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0	Trustix: http://http.trustix.org/pub/trustix/updates/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-504.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf** We are not aware of any exploits for this vulnerability.			**Avaya Se ASA-2005 14, 2006**
Multiple Vendors Linux Kernel; **Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0**	A vulnerability exists in the Linux kernel io_edgeport driver. A local user with a USB dongle can cause the kernel to crash or may be able to gain elevated privileges on the target system. The flaw resides in the edge_startup() function in 'drivers/usb/serial/io_edgeport.c'. Red Hat: https://bugzilla.redhat.com/bugzilla/attachment.cgi?id=107493&action=view Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel USB io_edgeport Driver Integer Overflow CVE Name: CAN-2004-1017	Low/ Medium (Medium if elevated privileges can be obtained)	SecurityT 1012477, 2004 Fedora U Notificatio FEDORA- January 3 **Avaya Se ASA-2005 14, 2006**
Multiple Vendors poppassd_ceti 1.0, poppassd_pam 1.0	A vulnerability exists in 'poppassd_pam' due to inadequate authentication before changing the system password, which could let a remote malicious user change any user's password and obtain superuser privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200501-22.xml There is no exploit required.	'poppassd_pam' Unauthorized Password Change CVE Name: CAN-2005-0002	High	Gentoo Li Advisory, January 1
Namazu Project Namazu 2.0.13 and prior	A vulnerability exists which can be exploited by malicious people to conduct Cross-Site Scripting attacks. Input passed to 'namazu.cgi' isn't properly sanitized before being returned to the user if the query begins from a tab ('%09'). This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Update to version 2.0.14: http://namazu.org/#download Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/n/namazu2/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Namazu Cross-Site Scripting Vulnerability CVE Name: CAN-2004-1318	High	Namazu S Decembe Debian S DSA 627- **SUSE Se Report, SUSE-SR January**
o3read 0.0.3	A vulnerability was reported in o3read. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted SXW file that, when processed by the target user with o3read, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the parse_html() function in 'o3read.c.' **Gentoo:** **http://security.gentoo.org/glsa/glsa-**	o3read parse_html() Buffer Overflow **CVE Name:** **CAN-2004-1288**	High	SecurityT 1012591, 2004 **Gentoo L GLSA 20 11, 2005**

	200501-20.xml A Proof of Concept exploit script has been published.			
OpenBSD OpenBSD 2.0-2.9, 3.0-3.6	A buffer overflow vulnerability exists in the 'mod_include' module due to insufficient validation of user-supplied tag strings length, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ Currently we are not aware of any exploits for this vulnerability.	OpenBSD httpd 'mod_include' Buffer Overflow	Low/High (High if arbitrary code can be executed)	SecurityF 2005
OpenBSD OpenBSD 2.0-2.9, 3.0-3.6	A remote Denial of Service vulnerability exists in the TCP timestamp processing functionality due to a failure to handle exceptional network data. Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ Currently we are not aware of any exploits for this vulnerability.	OpenBSD TCP Timestamp Remote Denial of Service	Low	SecurityT 1012861,
PHPGroupWare PHPGroupWare 0.9.16 RC1&2	A vulnerability exists in the 'acl_check' function, which could let a remote malicious user bypass the access control lists. Upgrades available at: http://download.phpgroupware.org/now There is no exploit code required.	PHPGroupWare 'ACL_Check' Access List Bypass	Medium	SecurityF 2005
PHPWind.Net PHPWind Board 1.3.6 & prior	A vulnerability exists in 'faq.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain/modify the administrator's password. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	PHPWind Administrator Password Modification	Medium	Securitea 2005
pizzashack.org rssh 2.2.2	A vulnerability exists which can be exploited to bypass certain security restrictions. The problem is that some of the predefined applications support flags, which allows command execution. This can be exploited to bypass the shell restriction and execute arbitrary commands. Gentoo: http://security.gentoo.org/glsa/glsa-200412-01.xml **Upgrade available at:** **http://prdownloads.sourceforge.net/rssh/rssh-2.2.3.tar.gz?download** Currently we are not aware of any exploits for this vulnerability.	pizzashack rssh Security Bypass	High	Secunia A SA13363, 2004 Gentoo Li Advisory, scponly, D **SecurityF 15, 2005**
RemoteSensing LibTIFF 3.5.7, 3.6.1, 3.7.0	Two vulnerabilities exist which can be exploited by malicious people to compromise a vulnerable system by executing arbitrary code. The vulnerabilities are caused due to an integer overflow in the "TIFFFetchStripThing()" function in "tif_dirread.c" when parsing TIFF files and"CheckMalloc()" function in "tif_dirread.c" and "tif_fax3.c" when handling data from a certain directory entry in the file header. Update to version 3.7.1: ftp://ftp.remotesensing.org/pub/libtiff/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://www.debian.org/security/2004/dsa-617 Gentoo: http://security.gentoo.org/glsa/glsa-200501-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE:** **ftp://ftp.suse.com/pub/suse/** **RedHat:** **http://rhn.redhat.com/errata/**	Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities CVE Name: CAN-2004-1308	High	iDEFENS Advisory Secunia S Decembe **SUSE Se Announc SUSE-SA January** **RedHat S RHSA-20 January** **US-Cert V Note, VU 14, 2005**

	RHSA-2005-019.html Currently we are not aware of any exploits for these vulnerabilities.			
SCO Unixware 7.1.1, 7.1.3, 7.1.4	A remote Denial of Service vulnerability exists when the 'mountd' service is registered in 'inetd.conf.' Patches available at: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.1/erg712731.711.pkg.Z There is no exploit required.	SCO UnixWare Mountd Remote Denial of Service CVE Name: CAN-2004-1039	Low	SCO Secu SCOSA-2 2005
Sergey Kiselev SGallery 1.0 1	Multiple vulnerabilities exist: a vulnerability exists in 'imageview.php' due to insufficient verification of input passed to the 'DOCUMENT_ROOT' parameter, which could let a remote malicious user execute arbitrary code; a vulnerability exists in 'imageview.php' due to insufficient sanitization of the 'idalbum' and 'idimage' parameters, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists if the 'idalbum' and 'idimage' variables are not set, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit required; however, a Proof of Concept exploit has been published.	SGallery Input Validation	Medium/ High (High if arbitrary code can be executed)	waraxe-2 January 1
SGI InPerson	A vulnerability exists in the 'SUN_TTSESSION_CMD' environment variable due to a design error, which could let a malicious user obtain superuser access. The vendor indicates that the product is no longer supported and no patch will be issued for this vulnerability. There is no exploit required; however, a Proof of Concept exploit has been published.	SGI InPerson Superuser Access	High	iDEFENS Advisory,
Squid-cache.org Squid 2.x	A remote Denial of Service vulnerability exists in the NTLM fakeauth_auth helper when running under a high load or for a long period of time, and a specially crafted NTLM type 3 message is submitted. Patch available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-fakeauth_auth.patch **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-25.xml** Currently we are not aware of any exploits for this vulnerability.	Squid NTLM fakeauth_auth Helper Remote Denial of Service	Low	Secunia A SA13789, **Gentoo L** **Advisor,** **January**
Squid-cache.org Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 .STABLE4&5, 2.4 .STABLE6&7, 2.4 .STABLE2, 2.4, 2.5 .STABLE3-7, 2.5 .STABLE1	Two vulnerabilities exist: remote Denial of Service vulnerability exists in the Web Cache Communication Protocol (WCCP) functionality due to a failure to handle unexpected network data; and buffer overflow vulnerability exists in the 'gopherToHTML()' function due to insufficient validation of user-supplied strings, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-wccp_denial_of_service.patch http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-gopher_html_parsing.patch Gentoo: http://security.gentoo.org/glsa/glsa-200501-25.xml There is no exploit required.	Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow	Low/High (High if arbitrary code can be executed)	Secunia A January 1
SquirrelMail Development Team SquirrelMail Vacation Plugin 0.14 -1.2rc2, 0.15 -1.43a	Two vulnerabilities exists in the 'ftpfile' program due to insufficient input validation, which could let a remote malicious user execute arbitrary commands with root privileges or obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits scripts have been published.	SquirrelMail Vacation Plugin 'FTPFile' Input Validation	Medium/ High High if arbitrary code can be executed)	LSS Secu LSS-2005 11, 2005

Steve Kirkendall Helvis 1.8	Multiple vulnerabilities exist: a vulnerability exists in the 'elvprsv' utility, which could let a malicious user delete arbitrary files; a vulnerability exists in the 'elvprsv' utility on preserved generated emails due to weak default permissions, which could let a malicious user obtain sensitive information; and a vulnerability exists in the 'elvrec' utility, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Steve Kirkendall Helvis elvprsv Arbitrary File Deletion & Sensitive Information Disclosure	Medium	SecurityF 2005
Sun Microsystems, Inc. Solaris 8.0 _x86, 8.0, 9.0 _x86, 9.0	A vulnerability exists in the Sun Solaris Management Console (SMC) Graphical User Interface due to a failure to create secure accounts that have no password, which could let a remote malicious user obtain unauthorized access. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57717-1&searchclause= There is no exploit required.	Solaris Management Console (SMC) Blank Passwords	Medium	Sun(sm) A 57717, Ja
Thibault Godouet Fcron 2.x	Multiple vulnerabilities exist: a vulnerability exists in the 'fcronsighup' utility due to a design error, which could let a malicious user obtain sensitive information; a vulnerability exists because the 'fcronsighup' utility can bypass access restrictions, which could let a malicious user supply arbitrary configuration settings; an input validation vulnerability exists in the 'fcronsighup' utility, which could let a malicious user delete arbitrary files; and a vulnerability exists because a malicious user can view the contents of the 'fcron.allow' and 'fcron.deny' files due to a file descriptor leak. Update available at: http://fcron.free.fr/download.php Gentoo: http://security.gentoo.org/glsa/glsa-200411-27.xml **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Thibault Godouet Fcron Multiple Vulnerabilities CVE Names: CAN-2004-1030 CAN-2004-1031 CAN-2004-1032 CAN-2004-1033	Medium	iDEFENS Advisory, 2004 Gentoo Li Advisory, Novembe **Trustix S Security TSLSA-2 13, 2005**
TWiki TWiki 20030201	A vulnerability exists in 'Search.pn' due to an input validation error when handling search requests, which could let a remote malicious user execute arbitrary commands. Hotfix available at: http://twiki.org/cgi-bin/view/Codev/SecurityAlertExecuteCommandsWithSearch Gentoo: http://security.gentoo.org/glsa/glsa-200411-33.xml **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** An exploit script has been published.	TWiki Search Shell Metacharacter Remote Arbitrary Command Execution CVE Name: CAN-2004-1037	High	Securitea 2004 PacketSto 2004 Gentoo Li Advisory, Novembe **Conectiv Announc CLA-2005 2005**
University of Cambridge Exim 4.40-4.43	A buffer overflow vulnerability exists in the 'dns_build_reverse()' function, which could let a malicious user execute arbitrary code. Patch available at: http://www.exim.org/mail-archives/exim-announce/2005/msg00000.html A Proof of Concept exploit has been published.	Exim 'dns_build_reverse()' Buffer Overflow	High	iDEFENS Advisory,
University of Minnesota gopherd 3.0.0-3.0.5	Multiple vulnerabilities exist due to insufficient sanitization of user-supplied input and a failure to verify input sizes, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/g/gopher/ Currently we are not aware of any exploits for these vulnerabilities.	University of Minnesota Gopher Multiple Remote Vulnerabilities	Low/High (High if arbitrary code can be executed)	Debian S DSA 638- 2005

VideoDB VideoDB 2.0 .0	Multiple vulnerabilities exist: a vulnerability exists due to insufficient sanitization of various input before being used in an SQL query, which could let a a remote malicious user inject arbitrary SQL code; a Cross-Site Scripting vulnerability exists due to insufficient sanitization of various input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in 'edit.php,' which could let a remote malicious user edit/delete arbitrary movie database entries. Upgrade available at: http://prdownloads.sourceforge.net/videodb/videodb-2_0_2.tgz?download Currently we are not aware of any exploits for these vulnerabilities.	VideoDB Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Secunia A SA13765,
VIM Development Group VIM 6.0-6.2, 6.3.011, 6.3.025, 6.3 .030, 6.3.044, 6.3 .045	Multiple vulnerabilities exist in 'tcltags' and 'vimspell.sh' due to the insecure creation of temporary files, which could let a malicious user corrupt arbitrary files. No workaround or patch available at time of publishing. There is no exploit required.	Vim Insecure Temporary File Creation	Medium	Secunia A SA13841,

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apple iTunes 4.2.72, 4.5-4.7	A buffer overflow vulnerability exists when handling '.m3u' and '.pls' playlists due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://www.apple.com/itunes/download/ Exploit scripts have been published.	Apple ITunes Playlist Buffer Overflow CVE Name: CAN-2005-0043	High	iDEFENSE Security Advisory, January 13, 2005 US-CERT Vulnerability Note, VU#377368, January 14, 2005
AWStats AWStats 5.0-5.9, 6.0-6.2	Several vulnerabilities exist: a vulnerability exists in the 'awstats.pl' script due to insufficient validation of the 'configdir' parameter, which could let a remote malicious user execute arbitrary code; and an unspecified input validation vulnerability exists. Upgrades available at: http://awstats.sourceforge.net/files/awstats-6.3.tgz Currently we are not aware of any exploits for these vulnerabilities.	AWStats Multiple Remote Input Validation	High	Securiteam, January 18, 2005
BiTSHiFTERS BiTBOARD 2.0, 2.5	A Cross-Site Scripting vulnerability exists in the BBCode 'IMG' tag due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	BiTBOARD Cross-Site Scripting	High	Bugtraq, January 12, 2005
BottomLine WebSeries Payment Application 4.0	Multiple vulnerabilities exist: a vulnerability exists because an authenticated user can access certain URLs directly to perform privileged actions; a vulnerability exists because HTTP variables disclose system information; an input validation vulnerability exists in 'BTInteractiveViewer.asp' when files and directories are enumerated via the 'ReportPath' and 'ReportName' parameters; an input validation vulnerability exists in the 'ReportPath' and 'ReportName' parameters, which could let a remote malicious user download and execute arbitrary reports; a vulnerability exists because a shorter password than permitted can be set; and a vulnerability exists because an authenticated malicious user can change other user's passwords. No workaround or patch available at time of publishing. There is no exploit required; however, a Proof of Concept exploit has been published.	BottomLine Webseries Payment Application Multiple Vulnerabilities	Medium	Portcullis Security Advisory, January 10, 2005

creamed-coconut.org SparkleBlog	Multiple vulnerabilities exist: a vulnerability exists in 'journal.php' due to insufficient sanitization of the 'id' parameter and in 'archives.php' due to insufficient sanitization of the 'year' parameter, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability exists in 'journal.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the 'admin' directory, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because a remote malicious user can supply a specially crafted URL to cause the system to disclose the installation path. No workaround or patch available at time of publishing. There is no exploit required; however, Proofs of Concept exploits have been published.	SparkleBlog Multiple Input Validation	Medium/ High (High if arbitrary code can be executed)	Bugtraq, January 15, 2005
Deutsche Telekom Teledat 530	A remote Denial of Service vulnerability exists due to a failure to handle exceptional conditions. No workaround or patch available at time of publishing. There is no exploit code required.	Deutsche Telekom Teledat 530 Remote Denial of Service	Low	Bugtraq, January 11, 2005
dokeos.com Dokeos Open Source Learning & Knowledge Management Tool 1.4, 1.5, 1.5.3-1.5.5	A Cross-Site Scripting vulnerability exists in the course description functionality due to insufficient sanitization, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit required.	Dokeos Course Description Cross-Site Scripting	High	Security Advisory B004, January 11, 2005
eMotion, Inc. MediaPartner Enterprise 5.0, 5.1	Multiple vulnerabilities exist: a vulnerability exists when handling requests for '.bhtml' files due to an input validation error, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'In Place Password Update' process, which could let a remote malicious user change arbitrary user's passwords; a Directory Traversal vulnerability exists due to insufficient input validation, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of input passed to the directory listing page, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Motion MediaPartner Enterprise Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA13820, January 17, 2005
GNU TikiWiki 1.7.9, 1.8.5, and 1.9dr4	A vulnerability exists in the uploading of image files. A remote authenticated user can execute arbitrary commands on the target system. A remote authenticated user with upload privileges can invoke the edit page to upload a PHP script to the 'img/wiki_up' directory instead of an image file. Then, the user can cause the web server to execute the script. The vendor has issued fixed versions (1.7.9, 1.8.5, and 1.9dr4), available at: http://sourceforge.net/project/showfiles.php?group_id=64258 **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-12.xml** Currently we are not aware of any exploits for this vulnerability.	GNU TikiWiki Pictures Lets Remote Users Execute Arbitrary Commands	High	TikiWiki Security Alert, December 12, 2004 **Gentoo Linux Security Advisory, GLSA 200501-12, January 10, 2005**
Horde Project Horde 3.0	Cross-Site Scripting vulnerabilities exist in 'index.php' due to insufficient sanitization of the 'url' parameter and in 'prefs.php' due to insufficient sanitization of the 'group' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://ftp.horde.org/pub/horde/horde-3.0.2.tar.gz There is no exploit required; however, Proofs of Concept exploits have been published.	Horde 'prefs.php' and 'index.php' Cross-Site Scripting	High	Hyperdose Security Advisory, January 13, 2005

JohnyTech Encrypted Messenger Plug-in 3.0.71	A remote Denial of Service vulnerability exists due to an error when processing incoming messages. No workaround or patch available at time of publishing. There is no exploit required.	JohnyTech Encrypted Messenger Plug-In Remote Denial of Service	Low	Secunia Advisory, SA13844, January 14, 2005
Lars Ellingsen Guestserver 5.0	A vulnerability exists in the 'message' parameter due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code or obtain the sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Guestserver Input Validation	Medium/ High (High if arbitrary code can be executed)	SYSTEMSECURE.ORG Advisory, 10012005, January 11, 2005
Minis Minis 0.x	A Directory Traversal vulnerability exists in 'minis.php' due to insufficient validation of the 'month' parameter, which could let a remote malicious user obtain sensitive information or cause a Denial of Service. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Minis Directory Traversal	Low/ Medium (Medium if sensitive information can be obtained)	Secunia Advisory, : SA13866, January 17, 2005
MPM PHP Scripts Guestbook 1.2, 1.5	A vulnerability exists in 'top.php' due to insufficient verification of the 'header' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	MPM Guestbook 'top.php' Input Validation	High	SYSTEMSECURE.ORG Advisory, January 13, 2005
Multiple Vendors Hitachi Directory Server 2.x; HP-UX B.11.00, B.11.11, B.11.23; Netscape Directory Server 6.21 & prior	A buffer overflow vulnerability exists when a specially crafted LDAP packet is submitted, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. Hitachi: http://www.hitachi-support.com/security_e/vuls_e/HS05-001_e/01-e.html HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBUX01105 Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor LDAP Directory Server Buffer Overflow	Low/High (High if arbitrary code can be executed)	US-CERT Vulnerability Note, VU#258905, January 14, 2005 Hitachi Security Advisory, HS05-001, January 12, 2005
Multiple Vendors Check Point Software FireWall-1 R55 HFA08 with SmartDefense; Internet Security Systems SiteProtector 2.0.4.561, 2.0 SP3; IronPort IronPort with Sophos AV Engine 3.88; McAfee Webshield 3000 4.3.20; TippingPoint Unity-One with Digital Vaccine 2.0.0.2070; Trend Micro InterScan Messaging Security Suite 3.81, 5.5, Trend Micro WebProtect 3.1	A security vulnerability exists due to a failure to decode base64-encoded images in 'data' URIs, which could lead to a false sense of security. No workaround or patch available at time of publishing. There is no exploit required.	Multiple Vendor Anti-Virus GatewayBase64 Encoded Image Decode Failure	Medium	Bugtraq, January 11, 2005

Multiple Vendors Debian Linux 3.0 spar, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.7	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the DICOM dissector; a remote Denial of Service vulnerability exists in the handling of RTP timestamps; a remote Denial of Service vulnerability exists in the HTTP dissector; and a remote Denial of Service vulnerability exists in the SMB dissector when a malicious user submits specially crafted SMB packets. Potentially these vulnerabilities may also allow the execution of arbitrary code. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200412-15.xml **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Multiple Denial of Service & Potential Code Execution Vulnerabilities CVE Names: CAN-2004-1139 CAN-2004-1140 CAN-2004-1141 CAN-2004-1142	Low/High (High if arbitrary code can be executed)	Ethereal Security Advisory, enpa-sa-00016, December 15, 2004 **Conectiva Linux Security Announcement, CLA-2005:916, January 13, 2005**
MySQL AB MaxDB 7.5.00.14-7.5.00.16, 7.5.00.12, 7.5.00.11, 7.5.00.08, 7.5.00	A buffer overflow vulnerability exists due to insufficient bounds checking in the websql CGI application, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://dev.mysql.com/downloads/maxdb/7.5.00.html Currently we are not aware of any exploits for this vulnerability.	MySQL MaxDB Remote Buffer Overflow	High	iDEFENSE Security Advisory, January 13, 2005
MySQL.com MySQL 4.x	A vulnerability exists in the 'mysqlaccess.sh' script because temporary files are created in an unsafe manner, which could let a malicious user obtain elevated privileges. Update available at: http://lists.mysql.com/internals/20600 Currently we are not aware of any exploits for this vulnerability.	MySQL 'mysqlaccess.sh' Unsafe Temporary Files CVE Name: CAN-2005-0004	Medium	SecurityTracker Alert, 1012914, January 17,2005
Netgear Netgear FVS318	Several vulnerabilities exist: a vulnerability exists because an URL that contains hex encoded characters may bypass an URL filter setup by the administrator; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of input passed to an URL that is blocked by an URL filter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	NETGEAR FVS318 Security Bypass & Cross Site Scripting	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA13787, January 17, 2005
NZEO Zeroboard 4.1, pl1-pl5	Multiple vulnerabilities exist: a vulnerability exists in the 'print_category.php' script due to insufficient validation of the 'dir' parameter, which could let a remote malicious user execute arbitrary PHP code; a vulnerability exists because a remote malicious user can submit a specially crafted URL to view files on the target system; and a vulnerability exists in several zero_vote scripts due to insufficient validation, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit required; however, Proofs of Concept exploits have been published.	Zeroboard Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	STG Security Advisor, SSA-20050113-25, January 13, 2005
PHP Gift Registry PHP Gift Registry 1.x	A vulnerability exists in 'index.php' due to insufficient sanitization of the 'messageid,' 'shopper,' and 'shopfor' parameters and in 'item.php' due to insufficient sanitization of the 'itemid' parameter, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHP Gift Registry Parameter Input Validation	High	Secunia Advisory, SA13873, January 17, 2005
PHP Group PHP 4.3.6-4.3.9, 5.0 candidate 1-canidate 3, 5.0 .0-5.0.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'pack()' function, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the 'unpack()' function, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'safe_mode' when executing commands, which could let a remote malicious user bypass the security restrictions; a vulnerability exists in 'safe_mode' combined with certain	PHP Multiple Remote Vulnerabilities CVE Names: CAN-2004-1018	Medium/ High (High if arbitrary code can	Bugtraq, December 16, 2004 **Conectiva Linux Security Announcement, CLA-2005:915,**

	implementations of 'realpath(),' which could let a remote malicious user bypass security restrictions; a vulnerability exists in 'realpath()' because filenames are truncated; a vulnerability exists in the 'unserialize()' function, which could let a remote malicious user obtain sensitive information or execute arbitrary code; a vulnerability exists in the 'shmop_write()' function, which may result in an attempt to write to an out-of-bounds memory location; a vulnerability exists in the 'addslashes()' function because '\0' if not escaped correctly; a vulnerability exists in the 'exif_read_data()' function when a long sectionname is used, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in 'magic_quotes_gpc,' which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.php.net/downloads.php Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required; however, a Proof of Concept exploit script has been published.	CAN-2004-1063 CAN-2004-1064 CAN-2004-1019 CAN-2004-1020 CAN-2004-1065	be executed)	**January 13, 2005**
Siteman Siteman 1.1.9	A Cross-Site Scripting vulnerability exists in the 'news.php' and 'forums.php' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Siteman Cross-Site Scripting	High	PersianHacker.NET Security Team Advisory, January 14, 2005
ViewCVS ViewCVS 0.9.2 & prior	A vulnerability exists because it is possible to access CVSROOT and forbidden directories via the tarball generation functionality, which could let malicious user bypass security restrictions. Debian: http://security.debian.org/pool/updates/main/v/viewcvs/ Gentoo: http://security.gentoo.org/glsa/glsa-200412-26.xml **SuSE:** **ftp://ftp.suse.com/pub/suse/** A Proof of Concept exploit has been published.	ViewCVS Ignores 'hide_cvsroot' and 'forbidden' Settings **CVE Name:** **CAN-2004-1062**	Medium	SecurityTracker Alert ID, 1012431, December 6, 2004 Gentoo Advisory GLSA 200412-26, December 28, 2004 **SUSE Security Summary Report, SUSE-SR:2005:001, January 12, 2005**
WoltLab Burning Board Lite 1.0 .0, 1.0.1e	An input validation vulnerability exists in the 'addentry.php' script, which could let a remote malicious user obtain or corruption sensitive database information. . No workaround or patch available at time of publishing. There is no exploit required	WoltLab Burning Board Lite 'addentry.php' Input Validation	High	Bugtraq, January 10, 2005

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	Script name	Workaround or Patch Available	Script Description

Order)			
January 18, 2005	files.zip injecthh_op_2-code_by_liudieyu.zip	Yes	Exploits for the Microsoft Windows HTML Help ActiveX Control vulnerability.
January 17, 2005	itunesPLS.txt itunesPLS-local.txt	Yes	Script that exploit the Apple ITunes Playlist Buffer Overflow vulnerability.
January 16, 2005	auth_radius.c	No	Script that exploits the Apache 'mod_auth_radius' Integer Overflow vulnerability.
January 16, 2005	breedzero.zip breed.tar	No	Proof of Concept exploit for the Brat Designs Breed Remote Denial of Service vulnerability.
January 16, 2005	exim.pl.txt eximExploit.tar.gz	Yes	Proof of Concept exploit for the Exim dns_build_reverse() Buffer Overflow vulnerability.
January 16, 2005	ExploitingFedora.txt	N/A	Whitepaper discussing how to exploit overflow vulnerabilities on Fedora Core 2.
January 16, 2005	fuzzer-1.1.tar.gz	N/A	A multi protocol fuzzing tool written in Python that can be used to find new SQL injection, format string, buffer overflow, directory traversal, and other vulnerabilities.
January 16, 2005	stackgrow2.c	Yes	Proof of Concept exploit for the Linux Kernel Symmetrical Multiprocessing Page Fault Superuser Privileges vulnerability.
January 16, 2005	vanisher.tgz	Yes	Proof of Concept exploit for the Windows ANI File Parsing vulnerability along with a complete detailed paper describing the process of creating it.
January 15, 2005	john-1.6.37.mscash.3.diff.gz	N/A	This patch is for john the ripper and adds the ability to crack MS Cached Credential hashes. To be used in conjunction with the Cachedump tool.
January 13, 2006	fm-eyetewnz.c atmaca.c	Yes	Scripts that exploit the Apple ITunes Playlist Buffer Overflow vulnerability.
January 13, 2005	anieeye.zip	Yes	Proof of Concept exploit for the Microsoft Windows ANI File Parsing Errors vulnerability.
January 13, 2005	stackgrow.c expand_stack.c	Yes	Proof of Concept exploits for the Linux Kernel Symmetrical Multiprocessing Page Fault Local Privilege Escalation vulnerability.
January 12, 2005	cachedump-1.0.zip	N/A	CacheDump is a tool that demonstrates how to recover cache entry information: username and hashed password (called MSCASH). This tool also explains the technical issues underneath Windows password cache entries, which are undocumented by Microsoft.
January 12, 2005	framework-2.3.tar.gz	N/A	The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code. The 2.3 release includes three user interfaces, 46 exploits and 68 payloads; many of these exploits are either the only ones publicly available or just much more reliable than anything else out there.
January 12, 2005	john-mspatch.1.3.37.2.diff.gz	N/A	This patch is for john the ripper and adds the ability to crack MS Cached Credential hashes. To be used in conjunction with the Cachedump tool.
January 12, 2005	LSS-2005-01-03.txt	No	Exploit for the SquirrelMail Vacation Plugin 'FTPFile' Input Validation vulnerability.
January 12, 2005	wins_ms04_045.pm	Yes	Exploit for the Microsoft WINS Name Validation vulnerability.
January 11, 2005	iis_w3who_overflow.pm	No	Exploit for the Microsoft Windows Resource Kit 'w3who.dll' Buffer Overflow & Input Validation vulnerability.
January 11, 2005	101_BXEC.c backupexec_ns.pm veritasABS.c	Yes	Exploits for the VERITAS Backup Exec Buffer Overflow vulnerability.
January 11, 2005	imail_imap_delete.pm	Yes	Exploit for the Ipswitch IMail Server Remote Buffer Overflow vulnerability.
January 11, 2005	webstar_ftp_user.pm	Yes	Exploit for the 4D WebSTAR Grants Access to Remote Users and Elevated Privileges to Local Users vulnerability.
January 10, 2005	mod_auth_radius_poc.c	No	A Proof of Concept exploit for the Apache mod_auth_radius Malformed RADIUS Server Reply Integer Overflow vulnerability.
January 10, 2005	Serv-U_2.5_DoS.pl	No	Perl script that exploits the RhinoSoft Serv-U FTP Server Remote Denial of Service vulnerability.
January 9, 2005	phpwind.pl	No	Perl script that exploits the PHPWind Board Remote File Include vulnerability.

[back to top]

Trends

- Nothing significant to report.

[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	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Sober-I	Win32 Worm	Increase	November 2004
3	Zafi-D	Win32 Worm	New to Table	December 2004
4	Zafi-B	Win32 Worm	Decrease	June 2004
5	Bagle-AA	Win32 Worm	Stable	April 2004
6	Bagle-AU	Win32 Worm	Decrease	October 2004
7	Netsky-D	Win32 Worm	Stable	March 2004
8	Netsky-Z	Win32 Worm	Return to Table	April 2004
9	Bagle.BB	Win32 Worm	Slight Decrease	September 2004
10	Netsky-Q	Win32 Worm	Slight Decrease	March 2004

Table Updated January 18, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Viruses or Trojans Considered to be a High Level of Threat**
    - The W32/VBSun-A worm spreads via email, tempting users into clicking onto its malicious attachment by pretending to be information about how to donate to a tsunami relief effort. However, running the attached file will not only forward the virus to other internet users but can also initiate a denial-of-service attack against a German hacking website. For more information see: http://www.sophos.com/virusinfo/articles/vbsuna.html

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
32/Baba-C		Win32 Worm
32/MyDoom-AA	W32/Mydoom.gen@MM W32.Mydoom.AI@mm MyDoom.AI W32/Mydoom.ap@MM W32.Mydoom.AI@mm MyDoom.AE	Win32 Worm
Backdoor.Abebot		Trojan

Backdoor.Globe		Trojan
Backdoor.IRC.Whisper.B	Backdoor.Win32.Delf.vb W32/Kassbot-A	Trojan
Backdoor.Lateda.B		Trojan
Backdoor.Omega		Trojan
Backdoor.Ranky.Q	TrojanProxy.Win32.Ranky.gen	Trojan
Backdoor.Ranky.R	Trojan-Proxy.Win32.Agent.cz Proxy-Piky	Trojan
Backdoor.Sdbot.AK		Win32 Worm
PWSteal.Lineage		Trojan
Troj/Multidr		Trojan
Trojan.Blubber		Trojan
Trojan.Netdepix.B		Trojan
Trojan.Wimad	Trojan-Downloader.WMA.Wimad.a Trojan-Downloader.WMA.Wimad.b Downloader-UA.a Downloader-UA.b Trojan.Wmvdown.A Trojan.Wmvdown.B	Trojan
VBS.Rowam.A		Trojan
W32.Linkbot.H	Backdoor.Win32.PoeBot.g	Win32 Worm
W32.Mugly.E@mm		Win32 Worm
W32.Mugly.F@mm		Win32 Worm
W32.Pejaybot		Win32 Worm
W32/Agobot-XB		Win32 Worm
W32/Anzae-A	WORM_ANZAE.A I-Worm.Pawur.a Tasin W32/Anzae.worm	Win32 Worm
W32/Baba-B	Worm.SomeFool.AJ-unp Email-Worm.Win32.Buchon.c W32/Buchon.c@MM W32/Buchon.c!keylog	Win32 Worm
W32/Bobax-D		Win32 Worm
W32/Forbot-DM	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Myfip-F	WORM_MYFIP.F W32/Myfip.worm.l Worm.Win32.Myfip.gen	Win32 Worm
W32/Rbot-AGZ		Win32 Worm
W32/Rbot-TF		Win32 Worm
W32/Rbot-TL		Win32 Worm
W32/Rbot-TP		Win32 Worm
W32/Rbot-TQ	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.w WORM_RBOT.AFK	Win32 Worm
W32/Rbot-TS		Win32 Worm
W32/Sdbot-TG		Win32 Worm
W32/Sdbot-TJ		Win32 Worm
W32/Sdbot-TO		Win32 Worm
W32/Wurmark-E		Win32 Worm
W97M.Temha		Word 97 Macro Virus
Win32.Formglieder.B	Win32/Formglieder.B.Trojan	Trojan
Win32.Lospad.C	Dialer-235 Dial/Conc-A W32/Dialer Win32.Lospad Win32/Lospad.C.Trojan Trojan.Win32.Dialer.gd	Win32 Worm

Win32.Mydoom.AH	Win32/Atak.Variant!Worm	Win32 Worm
Win32.Spybot.UY		IRC Bot
Win32.Tibick.C	P2P-Worm.Win32.Tibick.f	Win32 Worm
WORM_AGOBOT.AEK		Win32 Worm
WORM_BUCHON.C	W32/Buchon.gen@MM Win32/Buchon.B@mm I-Worm.Buchon.b	Win32 Worm
WORM_ZAR.A	Bloodhound.W32.VBWORM W32/Generic.a@MM !!! Win32/VBMassMail.gen+ Email-Worm.Win32.Zar.a W32/VBSun-A	Win32 Worm

[back to top]

Last updated January 19, 2005