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

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to 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
  - Alt-N WebAdmin Multiple Remote Vulnerabilities
  - AMAX Information Technologies, Inc. Magic Winmail Server Input Validation
  - Captaris Infinite Mobile Delivery Input Validation
  - Eternal Lines Web Server Remote Denial of Service
  - Eurofull E-Commerce 'mensresp.asp' Cross-Site Scripting
  - IceWarp Web Mail Multiple Remote
  - **INCA nProtect Gameguard Unauthorized Read/Write Access (Updated)**
  - **Microsoft Windows ANI File Parsing Errors (Updated)**
  - Nullsoft Winamp Variant IN_CDDA.dll Remote Buffer Overflow
  - SmarterMail Cross-Site Scripting
  - SnugServer FTP Service Directory Traversal
  - Techland Xpand Rally Remote Denial of Service
  - UR Software W32Dasm Remote Buffer Overflow
  - War FTP Daemon Remote Denial of Service
  - WebWasher Classic HTTP CONNECT Unauthorized Access
- UNIX / Linux Operating Systems
  - Alexander Barton ngIRCd Remote Buffer Overflow
  - **Apache Mod_Proxy Remote Buffer Overflow (Updated)**
  - **Apache mod_include Buffer Overflow (Updated)**
  - Apple ColorSync ICC Header Remote Buffer Overflow
  - **Apple Mac OS X 'at' Utility Information Disclosure (Updated)**
  - Apple Mail EMail Message ID Header Information Disclosure
  - **Apple Safari Open Windows Injection (Updated)**
  - **ARJ Software UNARJ Remote Buffer Overflow (Updated)**
  - Berlios GPSD Remote Format String
  - Black List Daemon select() Remote Buffer Overflow
  - Cadsoft.de VDR Daemon Remote File Overwrite
  - **Carnegie Mellon University Cyrus SASL Buffer Overflow & Input Validation (Updated)**
  - **Carsten Haitzler imlib Image Decoding Integer Overflow (Updated)**
  - Citadel/UX select() System Call Remote Buffer Overflow
  - David Gay F2C Multiple Insecure Temporary File Creation
  - Debian Pam Radius Auth File Information Disclosure
  - FireHOL Insecure Local Temporary File Creation
  - **FreeRADIUS Server Project Apache 'mod_auth_radius' Integer Overflow (Updated)**
  - **Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow (Updated)**
  - **GNU a2ps Filenames Shell Commands Execution (Updated)**
  - GNU CPIO Archiver Insecure File Creation
  - **GNU Vim / Gvim Modelines Command Execution Vulnerabilities (Updated)**
  - **GNU xine Buffer Overflow in pnm_get_chunk() (Updated)**
  - **GNU xine-lib Unspecified PNM and Real RTSP Clients Vulnerabilities (Updated)**
  - **GNU Xpdf Buffer Overflow in doImage() (Updated)**
  - HP-UX VirtualVault Remote Denial of Service
  - **ImageMagick Photoshop Document Buffer Overflow (Updated)**
  - **ImageMagick Remote EXIF Parsing Buffer Overflow (Updated)**
  - **Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow (Updated)**
  - Jabber select() Remote Buffer Overflow
  - **MPG123 Layer 2 Frame Header Buffer Overflow (Updated)**
  - **MPG123 Remote URL Open Buffer Overflow (Updated)**
  - Multiple Vendors Libdbi-perl Insecure Temporary File Creation
  - **Multiple Vendors IpTables Initialization Failure (Updated)**
  - **Multiple Vendors GNU Exim Buffer Overflows (Updated)**
  - **GNU Mailman Multiple Remote Vulnerabilities (Updated)**
  - **Multiple Vendors Gzip File Access (Updated)**
  - Multiple Vendors ISC BIND 'Q_UseDNS' Remote Denial of Service
  - Multiple Vendors BIND Validator Self Checking Remote Denial of Service
  - Multiple Vendors KDE Screensaver Lock Bypass
  - **Multiple Vendors Linux Kernel Auxiliary Message Layer State Error (Updated)**
  - **Multiple Vendors Linux Kernel IGMP Integer Underflow (Updated)**
  - **Multiple Vendors Linux Kernel 'sys32_ni_syscall' and 'sys32_vm86_warning' Buffer**

- **Mozilla Buffer Overflow in Processing NNTP URLs (Updated)**
- NEC Socks5 select() Remote Buffer Overflow
- Inferno Nettverk Dante select() Remote Buffer Overflow
- Novell iChain Authentication
- OpenH323 select() Remote Buffer Overflow
- PEiD Buffer Overflow Vulnerability
- **PHP Multiple Remote Vulnerabilities (Updated)**
- RealNetworks RealPlayer ActiveX Buffer Overflow
- Squid Error in Parsing HTTP Headers
- **SquirrelMail Cross-Site Scripting (Updated)**
- **Sun Java Plug-in Sandbox Security Bypass (Updated)**
- University of California PostgreSQL Multiple Vulnerabilities
- Xerox WorkCenter Pro Directory Traversal

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
Alt-N Technologies WebAdmin 3.0.2	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in 'useredit_account.wdm' due to insufficient sanitization of the 'user' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the 'useredit_account.wdm' script because an authenticated malicious user can edit other user's accounts; and a Cross-Site Scripting vulnerability exists in 'modalframe.wdm' due to insufficient sanitization of the 'file parameter, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://www.altn.com/download/default.asp?mode=1&Step=1&sProduct=WebAdmin&sLang=English&sFile=/Release/wa304_en.exe There is no exploit code required; however, Proofs of Concept exploits have been published.	Alt-N WebAdmin Multiple Remote Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Securiteam, January 31, 2005
AMAX Information Technologies Inc. Magic Winmail Server 4.0 (Build 1112)	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists in 'download.php' due to insufficient sanitization of the 'filename' parameter, which could let a remote malicious user obtain sensitive information; a Directory Traversal vulnerability exists in 'upload.php' due to insufficient sanitization of the 'filename' parameter, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists in 'userinfo.php' due to insufficient of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; an input validation vulnerability exists due the way IMAP commands are handled, which could let a remote malicious user modify system/user information; and a vulnerability exists because the 'PORT' command can be requested for arbitrary IP addresses, which could let a remote malicious user conduct port scanning of arbitrary hosts. Upgrades available at: http://www.magicwinmail.net/download/winmail.exe There is no exploit code required; however, Proofs of Concept exploits have been published.	Magic Winmail Server Input Validation	Medium/ High (High if arbitrary code can be executed)	SIG^2 Vulnerability Research Advisory, January 27, 2005

Captaris Infinite Mobile Delivery Webmail 2.6	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists because the installation path can be obtained. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Captaris Infinite Mobile Delivery Input Validation	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert, 1013044, January 31, 2005
EternalLines.com Eternal Lines Web Server 1.0	A remote Denial of Service vulnerability exists when a malicious user submits approximately 70 simultaneous connections to the target web server from the same originating host. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Eternal Lines Web Server Remote Denial of Service	Low	GSSIT Advisory, January 31, 2005
Eurofull E-Commerce	A Cross-Site Scripting vulnerability exists in the 'mensresp.asp' script due to insufficient validation of the 'nombre' parameter, 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.	Eurofull E-Commerce 'mensresp.asp' Cross-Site Scripting	High	Security .Net Information Advisore, January 31, 2005
IceWarp Web Mail 5.3	Multiple vulnerabilities exist: a vulnerability exists when accessing 'calendar_d.html,' 'calendar_m.html,' 'calendar_w.html,' and 'calendar_y.html' directly with a valid session ID in the 'id' parameter, which could let a remote malicious user obtain sensitive information; a vulnerability exists due to weak encryption of user credentials in the 'users.cfg,' 'settings.cfg,' 'user.dat,' and 'users.dat' files, which could let a malicious user obtain sensitive information; and multiple Cross-Site Scripting and HTML injection vulnerabilities exist 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.	IceWarp Web Mail Multiple Remote	Medium/ High (High if arbitrary code can be executed)	ShineShadow Security Report , January 29, 2005
INCA nProtect Gameguard	A vulnerability exists in the kernel driver functionality because the I/O permission mask can be modified, which could let an unauthorized malicious user obtain read/write access. No workaround or patch available at time of publishing. **Another Proof of Concept exploit script has been published.**	INCA nProtect Gameguard Unauthorized Read/Write Access	Medium	Bugtraq, January 17, 2005 **Bugtraq, January 28, 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 Bulletin V1.1 (January 20, 2005): Updated CAN reference and added acknowledgment to finder for CAN-2004-1305. **Another 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 Security Bulletin, MS05-002, V1.1, January 20, 2005 **PacketStorm, January 31, 2005**
NullSoft Winamp 5.01- 5.08	A buffer overflow vulnerability exists in the 'IN_CDDA.dll' library due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://forums.winamp.com/showthread.php?s=&threadid=202799 A Proof of Concept exploit script has been published.	Nullsoft Winamp Variant IN_CDDA.dll Remote Buffer Overflow CVE Name:	High	NSFOCUS Security Advisory, SA2005-01, January 27, 2005

		CAN-2004-1150		
SmarterTools Inc. SmarterMail	A Cross-Site Scripting vulnerability exists because attached files have a predictable URL and are placed inside the web root, which could let al remote malicious user execute arbitrary HTML and script code. Update available at: http://www.smartertools.com/Products/SmarterMail/DL/V2.aspx A Proof of Concept exploit has been published.	SmarterMail Cross-Site Scripting	High	Secunia Advisory, SA14080, January 31, 2005
SnugServer SnugServer 3.0.0.40	A Directory Traversal vulnerability exists due to an input validation error, which could let a remote malicious user obtain sensitive information. Update available at: http://www.snugserver.com/download.php There is no exploit code required.	SnugServer FTP Service Directory Traversal	Medium	Secunia Advisory, SA14063, January 28, 2005
Techland Xpand Rally 1.x	A remote Denial of Service vulnerability exists due to an unchecked memory allocation. Update available at: http://www.xpandrally.com/en/show.php?006 A Proof of Concept exploit script has been published.	Xpand Rally Remote Denial of Service	Low	Securiteam, February 1, 2005
URsoftware W32Dasm 8.94	A buffer overflow vulnerability exists due to insufficient validation of string length of files loaded for debugging, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	W32Dasm Remote Buffer Overflow	High	SecurityTracker Alert, 1012997, January 25, 2005
War FTP Daemon War FTP Daemon 1.8, 1.82 RC9	A remote Denial of Service vulnerability exist due to an error when handling 'CWD' commands. Upgrades available at: ftp://ftp.jgaa.com/pub/products/Windows/ WarFtpDaemon/1.7_Series/i386/ warftpd-1.82-00-RC10-i386.exe A Proof of Concept exploit script has been published.	War FTP Daemon Remote Denial of Service	Low	Secunia Advisory, SA14054, January 28, 2005
webwasher AG Webwasher Classic 2.2.1, 3.3 build 44, 3.3	A vulnerability exists due to a design error because connections to the local host interface are allowed by the proxy, which could let a remote malicious user bypass security restrictions. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proofs of Concept exploit has been published.	WebWasher Classic HTTP CONNECT Unauthorized Access	Medium	Secunia Advisory, SA14058, January 28, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Alexander Barton ngIRCd 0.6, 0.6.1, 0.7, 0.7.1, 0.7.5-0.7.7, 0.8, 0.8.1	A buffer overflow vulnerability exists in 'lists.c' in the 'Lists_MakeMask()' function due to insufficient boundary checks, which could let a remote malicious user cause a Denial or Service or obtain unauthorized access. Update available at: http://download.berlios.de/ngircd/ngircd-0.8.2.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200501-40.xml Currently we are not aware of any exploits for this vulnerability.	ngIRCd Remote Buffer Overflow	Low/ Medium (Medium if unauthorized access can be obtained)	Gentoo Linux Security Advisory, GLSA 200501-40, January 28,2005

Apache Software Foundation Conectiva Gentoo HP Immunix Mandrake OpenBSD OpenPKG RedHat SGI Trustix Apache 1.3.26-1.3.29, 1.3.31; OpenBSD –current, 3.4, 3.5	A buffer overflow vulnerability exists in Apache mod_proxy when a 'ContentLength:' header is submitted that contains a large negative value, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://marc.theaimsgroup.com/?l=apache-httpd-dev&m=108687304202140&q=p3 OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/apache-1.3.29-2.0.3.src.rpm Gentoo: http://security.gentoo.org/glsa/glsa-200406-16.xml Mandrake: http://www.mandrakesoft.com/security/advisories SGI: ftp://patches.sgi.com/support/free/security/ Fedora Legacy: http://download.fedoralegacy.org/redhat/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Apple: http://www.apple.com/swupdates/ **HP:** **http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01113** Currently we are not aware of any exploits for this vulnerability.	Apache Mod_Proxy Remote Buffer Overflow CVE Name: CAN-2004-0492	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert, 1010462, June 10, 2004 Gentoo Linux Security Advisory, GLSA 200406-16, June 22, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:065, June 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.029, June 11, 2004 SGI Security Advisory, 20040605-01-U, June 21, 2004 Fedora Legacy Update Advisory, FLSA:1737, October 14, 2004 US-Cert Vulnerability Note VU#541310, October 19, 2004 Slackware Security Advisory, SSA:2004-299-01, October 26, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0056, November 5, 2004 Turbolinux Security Announcement, November 18, 2004 Apple Security Advisory, APPLE-SA-2004-12-02, December 3, 2004 **Secunia Advisory, SA14081, January 31, 2005**
Apache Software Foundation Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.46, 1.3.7 -dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.29, 1.3.31	A buffer overflow vulnerability exists in the 'get_tag()' function, which could let a malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200411-03.xml Slackware: ftp://ftp.slackware.com/pub/slackware/s Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-600.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-010_RHSA-2004-600.pdf **HP:** **http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01113** Exploit scripts have been published.	Apache mod_include Buffer Overflow CVE Name: CAN-2004-0940	High	SecurityFocus, October 20, 2004 Slackware Security Advisory, SA:2004-305-01, November 1, 2004 Gentoo Linux Security Advisory, GLSA 200411-03, November 2, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0056, November 5, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:134, November 17,2004 Turbolinux Security Announcement, November 18, 2004 Red Hat Advisory: RHSA-2004:600-12, December 13, 2004 Avaya Security Advisory, ASA-2005-010, January 14, 2005 **Secunia Advisory, SA14081, January 31, 2005**

Apple Mac OS X 10.0 3, 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.7, 10.0, 10.1-10.1.5, Mac OS X Server 10.2-10.2.8, 10.3-10.3.7	A buffer overflow vulnerability exists in the International Color Consortium (ICC) color profile processing functionality due to insufficient validation of user-supplied data prior to copying it into static process buffers, which could let a remote malicious user execute arbitrary code. Update available at: http://www.apple.com/support/downloads/ Currently we are not aware of any exploits for this vulnerability.	Apple ColorSync ICC Header Remote Buffer Overflow CVE Name: CAN-2005-0126	High	Apple Security Update, APPLE-SA-2005-01-25, January 25, 2005 US-CERT Vulnerability Note, VU#980078, January 27, 2005
Apple Mac OS X 10.3-10.3.6, Mac OS X Server 10.3-10.3.6,	A vulnerability exists in the 'at' utility due to improper access controls on job schedule files, which could let a malicious user obtain sensitive information. **Apple: http://www.apple.com/support/downloads/** There is no exploit required; however, a Proof of Concept exploit has been published.	Apple Mac OS X 'at' Utility Information Disclosure **CVE Name: CAN-2005-0125**	Medium	Immunity Advisory, January 17, 2005 **Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005** **US-CERT Vulnerability Note, VU#678150, January 28, 2005**
Apple Mail	A vulnerability exists because the globally unique Ethernet MAC address is used in computing the Message-ID header in outgoing e-mail messages, which could let a remote malicious user obtain sensitive information. Update available at: http://www.apple.com/support/downloads/ There is no exploit required.	Apple Mail EMail Message ID Header Information Disclosure CVE Name: CAN-2005-0127	Medium	Apple Security Update, APPLE-SA-2005-01-25, January 25, 2005 US-CERT Vulnerability Note, VU#464662, January 31, 2005
Apple Safari 1.2.4	A vulnerability exists which could allow a remote malicious user to inject content into an open window in certain cases to spoof web site contents. If the target name of an open window is known, a remote user can create Javascript that, when loaded by the target user, will display arbitrary content in the opened window. A remote user can exploit this to spoof the content of potentially trusted web sites. **Apple: http://www.apple.com/support/downloads/** A Proof of Concept exploit has been published.	Apple Safari Open Windows Injection **CVE Name: CAN-2004-1314**	Medium	SecurityTracker Alert ID: 1012459, December 8, 2004 **Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005**
ARJ Software Inc. UNARJ 2.62-2.65	A buffer overflow vulnerability exists due to insufficient bounds checking on user-supplied strings, 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 Debian: http://security.debian.org/pool/updates/non-free/u/unarj/ **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-022_RHSA-2005-007.pdf** Currently we are not aware of any exploits for this vulnerability.	ARJ Software UNARJ Remote Buffer Overflow CVE Name: CAN-2004-0947	High	SecurityTracker Alert I,: 1012194, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-29, November 19, 2004 SUSE Security Summary Report SUSE-SR:2004:003, December 7, 2004 Fedora Update Notification FEDORA-2004-414, December 11, 2004 RedHat Security Advisory, RHSA-2005:007-05, January 12, 2005 Debian Security Advisory, DSA 652-1, January 21, 2005 **Avaya Security Advisory, ASA-2005-022, January 25, 2005**
Berlios gpsd 1.10, 1.20, 1.90	A format string vulnerability exists in the 'gpsd_report()' function, 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.	Berlios GPSD Remote Format String	High	Securiteam, January 26, 2005

Black List Daemon bld 0.3	A buffer overflow vulnerability exists due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. No workaround or patch available at time of publishing. An exploit has been published but has not been released to the public.	Black List Daemon select() Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bugtraq, January 24, 2005
cadsoft.de vdr daemon 1.0	A vulnerability exists in 'dvbapi.c' because files are created in an unsafe manner, which c could let a remote malicious user overwrite arbitrary files. Debian: http://security.debian.org/pool/updates/main/v/vdr/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-42.xml Currently we are not aware of any exploits for this vulnerability.	VDR Daemon Remote File Overwrite CVE Name: CAN-2005-0071	Medium	Debian Security Advisory, DSA 656-1, January 25, 2005 Gentoo Linux Security Advisory, GLSA 200501-42, January 30,2005
Carnegie Mellon University Cyrus SASL 1.5.24, 1.5.27, 1.5.28, 2.1.9-2.1.18	Several vulnerabilities exist: a buffer overflow vulnerability exists in 'digestmda5.c,' which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'SASL_PATH' environment variable, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-546.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/c/cyrus-sasl/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **OpenPGK:** **ftp ftp.openpkg.org** Currently we are not aware of any exploits for these vulnerabilities.	Cyrus SASL Buffer Overflow & Input Validation CVE Name: CAN-2004-0884	High	SecurityTracker Alert ID: 1011568, October 7, 2004 Debian Security Advisories DSA 563-2, 563-3, & 568-1, October 12 , 14, & 16, 2004 Conectiva Linux Security Announcement, CLA-2004:889, November 11, 2004 **OpenPKG Security Advisory, OpenPKG Security Advisory, January 28, 2005**
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 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 TurboLinux: http://www.turbolinux.com/update/	Carsten Haitzler imlib Image Decoding Integer Overflow CVE Name: CAN-2004-1026 CAN-2004-1025	High	Secunia Advisory ID, SA13381, December 7, 2004 Red Hat Advisory, RHSA-2004:651-03, December 10, 2004 SecurityFocus, December 14, 2004 Debian DSA-618-1 imlib, December 24, 2004 Mandrakelinux Security Update Advisory, MDKSA-2005:007, January 12, 2005 Turbolinux Security Announcement, January 20, 2005 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**

	SUSE: **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.			
Citadel/UX Citadel/UX 5.90, 5.91, 6.08, 6.0 7, 6.23, 6.24, 6.26, 6.27	A buffer overflow vulnerability exists due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. Upgrades available at: http://easyinstall.citadel.org/citadel-6.30.tar.gz An exploit has been published but has not been released to the public.	Citadel/UX select() System Call Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bugtraq, January 24, 2005
David M. Gay f2c Fortran 77 Translator 1.3.1	Several vulnerabilities exist due to the insecure creation of temporary files, which could let a malicious user modify information or obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/f/f2c/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-43.xml There is no exploit required.	F2C Multiple Insecure Temporary File Creation CVE Names: CAN-2005-0017 CAN-2005-0018	Medium	Debian Security Advisory, DSA 661-1, January 27, 2005 Gentoo Linux Security Advisory GLSA 200501-43, January 30, 2005
Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A vulnerability exists because during installation a PAM radius configuration file is set world-readable, which could let a malicious user obtain sensitive information. Upgrades available at: http://security.debian.org/pool/updates/main/libp/ There is no exploit required.	Debian Pam Radius Auth File Information Disclosure CVE Name: CAN-2004-1340	Medium	Debian Security Advisory, DSA 659-1, January 26, 2005
FireHOL FireHOL 1.214	A vulnerability exists due to the insecure creation of various temporary files, which could let a malicious user overwrite arbitrary files. Update available at: http://firehol.sourceforge.net/ There is no exploit required	FireHOL Insecure Local Temporary File Creation	Medium	Secunia Advisory, SA13970, January 25, 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. **Debian:** **http://security.debian.org/pool/updates/main/libp/libpam-radius-auth/** A Proof of Concept exploit has been published.	FreeRADIUS Server Project Apache 'mod_auth_radius' Integer Overflow **CVE Name:** **CAN-2005-0108**	Low/High (High if arbitrary code can be executed)	LSS Security Advisory, LSS-2005-01-02, January 10, 2005 **Debian Security Advisory, DSA 659-1, January 26, 2005**
Glyph and Cog XPDF prior to 3.00pl3	A buffer overflow vulnerability exists in ' 'xpdf/Decrypt.cc' due to a boundary error in the 'Decrypt::makeFileKey2' function, which could let a remote malicious user execute arbitrary code. Update available at: http://www.foolabs.com/xpdf/download.html Patch available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch Debian: http://security.debian.org/pool/updates/main/c/cupsys/ http://security.debian.org/pool/updates/main/x/xpdf/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/ KDE: ftp://ftp.kde.org/pub/kde/security_patches Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/**	Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow CVE Name: CAN-2005-0064	High	iDEFENSE Security Advisory, January 18, 2005 **Conectiva Linux Security Announcement, CLA-2005:921, January 25, 2005** **Mandrakelinux Security Update Advisories, MDKSA-2005:016-021, January 26, 2005** **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**

	Mandrake: **http://www.mandrakesecure.net/en/ftp.php** **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.			
GNU a2ps 4.13	A vulnerability exists that could allow a malicious user to execute arbitrary shell commands on the target system. a2ps will execute shell commands contained within filenames. A user can create a specially crafted filename that, when processed by a2ps, will execute shell commands with the privileges of the a2ps process. A patch for FreeBSD is available at: http://www.freebsd.org/cgi/cvsweb.cgi/~checkout~/ports/ print/a2ps-letter/files/patch-select.c?rev=1.1&content-type=text/plain Debian: http://www.debian.org/security/2004/dsa-612 Gentoo: http://security.gentoo.org/glsa/glsa-200501-02.xml OpenPKG: ftp://ftp.openpkg.org/release/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** A Proof of Concept exploit has been published.	GNU a2ps Filenames Shell Commands Execution	High	SecurityTracker Alert ID, 1012475, December 10, 2004 Debian Security Advisory DSA-612-1 a2ps, December 20, 2004 Gentoo GLSA 200501-02, January 5, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.003, January 17, 2005 **Turbolinux Security Advisory, TLSA-2005-8, January 26, 2005**
GNU cpio 1.0, 1.1, 1.2	A vulnerability exists in 'cpio/main.c' due to a failure to create files securely, which could let a malicious user obtain sensitive information. Upgrades available at: http://ftp.gnu.org/gnu/cpio/cpio-2.6.tar.gz There is no exploit required.	CPIO Archiver Insecure File Creation CVE Name: CAN-1999-1572	Medium	SecurityTracker Alert, 1013041, January 30, 2005
GNU Vim 6.x, GVim 6.x; **Avaya Converged Communications Server 2.0, CVLAN, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing, 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 which can be exploited by local malicious users to gain escalated privileges. The vulnerabilities are caused due to some errors in the modelines options. This can be exploited to execute shell commands when a malicious file is opened. Successful exploitation can lead to escalated privileges but requires that modelines is enabled. Apply patch for vim 6.3: ftp://ftp.vim.org/pub/vim/patches/6.3/6.3.045 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-10.xml Red Hat: http://rhn.redhat.com/errata/RHSA-2005-010.html Mandrake: http://www.mandrakesoft.com/security/advisories **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-020_RHSA-2005-019.pdf** Currently we are not aware of any exploits for these vulnerabilities.	GNU Vim / Gvim Modelines Command Execution Vulnerabilities CVE Name: CAN-2004-1138	Medium	Gentoo Linux Security Advisory, GLSA 200412-10 / vim, December 15, 2004 Red Hat Advisory RHSA-2005:010-05, January 5, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:003, January 6, 2005 **Avaya Security Advisory, ASA-2005-020, January 25, 2005**
GNU xine prior to 0.99.3	Multiple vulnerabilities exist that could allow a remote user to execute arbitrary code on the target user's system. There is a buffer overflow in pnm_get_chunk() in the processing of the RMF_TAG, DATA_TAG, PROP_TAG, MDPR_TAG, and CONT_TAG parameters. The vendor has issued a fixed version of xine-lib (1-rc8), available at: http://xinehq.de/index.php/releases A patch is also available at: http://cvs.sourceforge.net/viewcvs.py/xine/xine-lib/src/input/pnm.c?r1=1.20&r2=1.21 Conectiva:	GNU xine Buffer Overflow in pnm_get_chunk() CVE Name: CAN-2004-1187 CAN-2004-1188	High	iDEFENSE Security Advisory 12.21.04 Gentoo, GLSA 200501-07, January 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:011, January 19, 2005 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**

	ftp://atualizacoes.conectiva.com.br/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-07.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** A Proof of Concept exploit has been published.			
GNU xine-lib 1.x	Multiple vulnerabilities with unknown impacts exist due to errors in the PNM and Real RTSP clients. Update to version 1-rc8: http://xinehq.de/index.php/download Gentoo: http://security.gentoo.org/glsa/glsa-200501-07.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	GNU xine-lib Unspecified PNM & Real RTSP Clients Vulnerabilities CVE Name: CAN-2004-1300	Not Specified	Secunia Advisory, SA13496, December 16, 2004 Gentoo Linux Security Advisory, GLSA 200501-07, January 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:011, January 19, 2005 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**
GNU Xpdf prior to 3.00pl2	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user. A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html A patch is available: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch KDE: http://www.kde.org/info/security/advisory-20041223-1.txt Gentoo: http://security.gentoo.org/glsa/glsa-200412-24.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ Mandrakesoft (update for koffice): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:165 Mandrakesoft (update for kdegraphics): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:163 Mandrakesoft (update for gpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:162 Mandrakesoft (update for xpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:161 Mandrakesoft (update for tetex): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:166 Debian: http://www.debian.org/security/2004/dsa-619 Fedora (update for tetex): http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Fedora:	GNU Xpdf Buffer Overflow in doImage() CVE Name: CAN-2004-1125	High	iDEFENSE Security Advisory 12.21.04 KDE Security Advisory, December 23, 2004 Mandrakesoft, MDKSA-2004:161,162,163,165, 166, December 29, 2004 Fedora Update Notification, FEDORA-2004-585, January 6, 2005 Gentoo Linux Security Advisory, GLSA 200501-13, January 10, 2005 **Conectiva Linux Security Announcement, CLA-2005:921, January 25, 2005** **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005** **Avaya Security Advisory, ASA-2005-027, January 25, 2005**

	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-13.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: http://support.sgi.com/browse_request/linux_patches_by_os **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.			
Hewlett-Packard Company VirtualVault A.04.70, A.04.60, A.04.50	A remote Denial of Service vulnerability exists due to a failure to handle malformed network data. Patches available at: http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01111 Currently we are not aware of any exploits for this vulnerability.	HP-UX VirtualVault Remote Denial of Service	Low	HP Security Bulletin, HPSBUX01111, January 26, 2005
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 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-26.xml **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-37.xml** Currently we are not aware of any exploits for this vulnerability.	ImageMagick Photoshop Document Buffer Overflow CVE Name: CAN-2005-0005	High	iDEFENSE Security Advisory, January 17, 2005 Ubuntu Security Notice, USN-62-1, January 18, 2005 Debian Security Advisory, DSA 646-1, January 19, 2005 Gentoo Linux Security Advisory, GLSA 200501-26, January 20, 2005 **Gentoo Linux Security Advisory, GLSA 200501-37, January 26, 2005**
ImageMagick ImageMagick 5.3.3, 5.4.3, 5.4.4.5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0, 6.0.1, 6.0.3-6.0.8	A buffer overflow vulnerability exists in the 'EXIF' parsing routine due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=24099 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-11.xml Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ SUSE: ftp://ftp.SUSE.com/pub/SUSE/i386/update/ Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:143 (Red Hat has re-issued it's update.)	ImageMagick Remote EXIF Parsing Buffer Overflow CVE Names: CAN-2004-0827 CAN-2004-0981	High	SecurityTracker Alert ID, 1011946, October 26, 2004 Gentoo Linux Security Advisory, GLSA 200411-11:01, November 6, 2004 Debian Security Advisory DSA 593-1, November 16, 2004 SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004 SUSE Security Summary Report, USE-SR:2004:001, November 24, 2004 Mandrakesoft Security Advisory, MDKSA-2004:143, December 6, 2004 Red Hat Security Advisory, RHSA-2004:636-03, December 8, 2004 **Turbolinux Security Advisory,**

	http://rhn.redhat.com/errata/RHSA-2004-480.html **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.			**TLSA-2005-7, January 26, 2005**
Info-ZIP Zip 2.3; **Avaya CVLAN, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing**	A buffer overflow vulnerability exists due to a boundary error when doing recursive compression of directories with 'zip,' which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zip/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE Red Hat: http://rhn.redhat.com/errata/RHSA-2004-634.html Debian: http://www.debian.org/security/2005/dsa-624 **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-019_RHSA-2004-634.pdf** Currently we are not aware of any exploits for this vulnerability.	Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow CVE Name: CAN-2004-1010	High	Bugtraq, November 3, 2004 Ubuntu Security Notice, USN-18-1, November 5, 2004 Fedora Update Notification, FEDORA-2004-399 & FEDORA-2004-400, November 8 & 9, 2004 Gentoo Linux Security Advisory, GLSA 200411-16, November 9, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:141, November 26, 2004 SUSE Security Summary Report, SUSE-SR:2004:003, December 7, 2004 Red Hat Advisory, RHSA-2004:634-08, December 16, 2004 Debian DSA-624-1, January 5, 2005 **Turbolinux Security Announcement, 20050131, January 31, 2005** **Avaya Security Advisory, ASA-2005-019, January 25, 2005**
JabberStudio jabberd 1.4.1	A buffer overflow vulnerability exists due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. No workaround or patch available at time of publishing. An exploit has been published but has not been released to the public.	Jabber select() Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bugtraq, January 24, 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: http://security.gentoo.org/glsa/glsa-200501-14.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	MPG123 Layer 2 Frame Header Buffer Overflow CVE Name: CAN-2004-0991	High	Gentoo Linux Security Advisory, GLSA 200501-14, January 11, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:009, January 19, 2005 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**
mpg123.de mpg123 pre0.59s, 0.59r	A buffer overflow vulnerability exists in the 'getauthfromURL()' function due to a boundary error, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/non-free/m/mpg123/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-27.xml **SUSE:**	MPG123 Remote URL Open Buffer Overflow CVE Name: CAN-2004-0982	High	Securiteam, October 21, 2004 Gentoo Linux Security Advisory, GLSA 200410-27, October 27, 2004 Debian Security Advisory, DSA 578-1 , November 1, 2004 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**

	ftp://ftp.SUSE.com/pub/SUSE A Proof of Concept exploit has been published.			
Multiple Vendors Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4, rc1-rc3; libdbi-perl libdbi-perl 1.21, 1.42	A vulnerability exists libdbi-perl due to the insecure creation of temporary files, which could let a remote malicious user overwrite arbitrary files. Debian: http://security.debian.org/pool/updates/main/libd/libdbi-perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-069.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libd/libdbi-perl/ There is no exploit required.	Libdbi-perl Insecure Temporary File Creation CVE Name: CAN-2005-0077	Medium	Debian Security Advisory, DSA 658-1, January 25, 2005 Ubuntu Security Notice, USN-70-1, January 25, 2005 Gentoo Linux Security Advisory, GLSA 200501-38, January 26, 2005 RedHat Security Advisory, RHSA-2005:069-08, February 1, 2005
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, 0 ia-64, ia-32, hppa, arm, alpha; Linux kernel 2.0.2, 2.4-2.4.26, 2.6-2.6.9	A vulnerability exists in 'iptables.c' and 'ip6tables.c' due to a failure to load the required modules, which could lead to a false sense of security because firewall rules may not always be loaded. Debian: http://security.debian.org/pool/updates/main/i/iptables/i Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ SUSE: ftp.SUSE.com/pub/SUSE **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit required.	IpTables Initialization Failure CVE Name: CAN-2004-0986	Medium	Debian Security Advisory, DSA 580-1 , November 1, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:125, November 4, 2004 SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004 Fedora Update Notification, FEDORA-2004-417, December 1, 2004 **Turbolinux Security Advisory, TLSA-2005-10, January 26, 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/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	GNU Exim Buffer Overflows CVE Names: CAN-2005-0021 CAN-2005-0022	High	SecurityTracker Alert ID: 1012771, January 5, 2005 Gentoo Linux Security Advisory, GLSA 200501-23, January 12, 2005 Debian Security Advisory, DSA 635-1 & 637-1, January 12 & 13, 2005 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005** **US-CERT Vulnerability Note, VU#132992, January 28, 2005**

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/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-29.xml **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	GNU Mailman Multiple Remote Vulnerabilities CVE Names: CAN-2004-1143 CAN-2004-1177	Medium/ High (High if arbitrary code can be executed)	SecurityTracker, January 12, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:015, January 25, 2005** **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**
Multiple Vendors gzip	A vulnerability exists in the gzip(1) command, which could let a malicious user access the files of other users that were processed using gzip. Sun Solaris: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57600-1 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:142 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Debian: http://www.debian.org/security/2004/dsa-588 **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Gzip File Access CVE Name: CAN-2204-0970	Medium	Sun(sm) Alert Notification, 57600, October 1, 2004 US-CERT Vulnerability Note VU#635998, October 18, 2004 Mandrakesoft Security Advisory, MDKSA-2004:142, December 6, 2004 Trustix Advisory TSL-2004-0050, September 30, 2004 Debian Security Advisory DSA 588-1, November 8, 2004 **Turbolinux Security Advisory, TLSA-2005-9, January 26, 2005**
Multiple Vendors ISC BIND 8.4.4, 8.4.5	A remote Denial of Service vulnerability exists in the 'q_usedns' array due to in sufficient validation of the length of user-supplied input prior to copying it into static process buffers. This could possibly lead to the execution of arbitrary code. Upgrade available at: http://www.isc.org/index.pl?/sw/bind/ Currently we are not aware of any exploits for this vulnerability.	ISC BIND 'Q_UseDNS' Remote Denial of Service CVE Name: CAN-2005-0033	Low/High (High if arbitrary code can be executed)	US-CERT Vulnerability Note, VU#327633, January 25, 2005
Multiple Vendors ISC BIND 9.3; MandrakeSoft Linux Mandrake 10.1 X86_64, 10.1	A remote Denial of Service vulnerability exists in the 'authvalidated()' function due to an error in the validator. Upgrade available at: http://www.isc.org/index.pl Mandrake: http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.	BIND Validator Self Checking Remote Denial of Service CVE Name: CAN-2005-0034	Low	US-CERT Vulnerability Note. VU#938617, January 25, 2005
Multiple Vendors KDE 2.0, BETA, 2.0.1, 2.1-2.1.2, 2.2-2.2.2	A vulnerability exists in 'kdesktop/lockeng.cc' and 'kdesktop/lockdlg.cc' due to insufficient return value checking, which could let a malicious user bypass the screensaver lock mechanism. Debian: http://security.debian.org/pool/updates/main/k/kdebase/ Currently we are not aware of any exploits for this vulnerability.	KDE Screensaver Lock Bypass CVE Name: CAN-2005-0078	Medium	Debian Security Advisory, DSA 660-1, January 26, 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-2004-549RHSA-2004-505RHSA-2004-689.pdf **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** 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 Security Research Advisory 0019, December 14, 2004 SecurityFocus, December 25, 2004 Secunia, SA13706, January 4, 2005 Avaya Security Advisory, ASA-2005-006, January 14, 2006 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
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 **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** 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 Security Research Advisory 0018, December 14, 2004 SecurityFocus, December 25, 2005 Secunia, SA13706, January 4, 2005 Avaya Security Advisory, ASA-2005-006, January 14, 2006 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**

Multiple Vendors Linux Kernel 2.6.x	Some potential vulnerabilities exist with an unknown impact in the Linux Kernel. The vulnerabilities are caused due to boundary errors within the 'sys32_ni_syscall()' and 'sys32_vm86_warning()' functions and can be exploited to cause buffer overflows. Immediate consequences of exploitation of this vulnerability could be a kernel panic. It is not currently known whether this vulnerability may be leveraged to provide for execution of arbitrary code. Patches are available at: http://linux.bkbits.net:8080/linux-2.6/cset@1.2079 http://linux.bkbits.net:8080/linux-2.6/gnupatch@41ae6af1cR3mJYIW6D8EHxCKSxuJiQ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel 'sys32_ni_syscall' and 'sys32_vm86_warning' Buffer Overflows CVE Name: CAN-2004-1151	Low/High (High if arbitrary code can be executed)	Secunia Advisory ID, SA13410, December 9, 2004 SecurityFocus, December 14, 2004 SecurityFocus, December 25, 2004 Secunia, SA13706, January 4, 2005 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
Multiple Vendors Linux Kernel versions except 2.6.9	A race condition vulnerability exists in the Linux Kernel terminal subsystem. This issue is related to terminal locking and is exposed when a remote malicious user connects to the computer through a PPP dialup port. When the remote user issues the switch from console to PPP, there is a small window of opportunity to send data that will trigger the vulnerability. This may cause a Denial of Service. This issue has been addressed in version 2.6.9 of the Linux Kernel. Patches are also available for 2.4.x releases: http://www.kernel.org/pub/linux/kernel/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Terminal Locking Race Condition CVE Name: CAN-2004-0814	Low	SecurityFocus, December 14, 2004 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
Multiple Vendors Linux Kernel versions except 2.6.9	The Linux Kernel is prone to a local vulnerability in the terminal subsystem. Reportedly, this issue can be triggered by issuing a TIOCSETD ioctl to a terminal interface at the moment a read or write operation is being performed by another thread. This could result in a Denial of Service or allow kernel memory to be read. This issue has been addressed in version 2.6.9 of the Linux Kernel. Patches are also available for 2.4.x releases: http://www.kernel.org/pub/linux/kernel/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel TIOCSETD Terminal Subsystem Race Condition CVE Name: CAN-2004-0814	Low	SecurityFocus, December 14, 2004 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
Multiple Vendors MandrakeSoft Corporate Server 3.0, x86_64, Linux Mandrake 10.0, AMD64, 10.1, X86_64;Novell Evolution 2.0.2l Ubuntu Linux 4.1 ppc, ia64, ia32; Ximian Evolution 1.0.3-1.0.8, 1.1.1, 1.2-1.2.4, 1.3.2 (beta)	A buffer overflow vulnerability exists in the main() function of the 'camel-lock-helper.c' source file, which could let a remote malicious user execute arbitrary code. Update available at: http://cvs.gnome.org/viewcvs/evolution/camel/camel-lock-helper.c?rev=1.7&hideattic=0&view=log Gentoo: http://security.gentoo.org/glsa/glsa-200501-35.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php	Evolution Camel-Lock-Helper Application Remote Buffer Overflow CVE Name: CAN-2005-0102	High	Gentoo Linux Security Advisory, GLSA 200501-35, January 25, 2005 Ubuntu Security Notice, USN-69-1, January 25, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:024, January 27, 2005

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ 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 **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-38.xml** 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 Security Notice, USN-44-1, December 21, 2004 Debian Security Advisory, DSA 620-1, December 30, 2004 OpenPKG Security Advisory, OpenPKG-SA-2005.001, January 11, 2005 **Gentoo Linux Security Advisory, GLSA 200501-38, January 26, 2005**
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.20; Gentoo Linux; GNOME GPdf 0.112; KDE KDE 3.2-3.2.3, 3.3, 3.3.1, kpdf 3.2; RedHat Fedora Core2; Ubuntu ubuntu 4.1, ppc, ia64, ia32, Xpdf Xpdf 0.90-0.93; 1.0.1, 1.0 0a, 1.0, 2.0 3, 2.0 1, 2.0, 3.0, SUSE Linux - all versions	Several integer overflow vulnerabilities exist in 'pdftops/Catalog.cc' and 'pdftops/XRef.cc,' which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/c/cupsys/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-20.xml KDE: ftp://ftp.kde.org/pub/kde/security_patches/post-3.3.1-kdegraphics.diff Mandrake: http://www.mandrakesecure.net/en/ftp.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/t/tetex-bin/ SUSE: Update: ftp://ftp.SUSE.com/pub/SUSE **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-31.xml** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows CVE Names: CAN-2004-0888 CAN-2004-0889	High	SecurityTracker Alert ID, 1011865, October 21, 2004 Conectiva Linux Security Announcement, CLA-2004:886, November 8, 2004 Debian Security Advisory, DSA 599-1, November 25, 2004 SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004 **Gentoo Linux Security Advisory, GLSA 200501-31, January 23, 2005**
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux;	A vulnerability exists in the tiffdump utility, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Fedora: http://download.fedora.redhat.com/pub/	LibTIFF TIFFDUMP Heap Corruption Integer Overflow CVE Name: CAN-2004-1183	High	SecurityTracker Alert ID, 1012785, January 6, 2005 RedHat Security Advisory, RHSA-2005:019-11, January 13, 2005 SGI Security Advisory, 20050101-01-U, January 19,

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; **Avaya CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0**	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 SGI: http://support.sgi.com/browse_request/linux_patches_by_os TurboLinux: http://www.turbolinux.com/update/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-021_RHSA-2005-019.pdf** Currently we are not aware of any exploits for this vulnerability.		2005 Turbolinux Security Announcement, January 20, 2005 Conectiva Linux Security Announcement, CLA-2005:920, January 20, 2005 **Avaya Security Advisory, ASA-2005-021, January 25, 2005**

Multiple Vendors Enlightenment Imlib2 1.0-1.0.5, 1.1, 1.1.1; ImageMagick ImageMagick 5.4.3, 5.4.4 .5, 5.4.8 .2-1.1.0 , 5.5.3 .2-1.2.0, 5.5.6 .0-2003040, 5.5.7,6.0.2; Imlib Imlib 1.9-1.9.14	Multiple buffer overflow vulnerabilities exist in the Iimlib/Imlib2 libraries when handling malformed bitmap images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Imlib: http://cvs.sourceforge.net/viewcvs.py/enlightenment/e17/ ImageMagick: http://www.imagemagick.org/www/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200409-12.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-465.html SUSE: ftp://ftp.SUSE.com/pub/SUSE/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57648-1&searchclause= http://sunsolve.sun.com/search/document.do?assetkey=1-26-57645-1&searchclause= TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-480.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/i RedHat: http://rhn.redhat.com/errata/RHSA-2004-636.html **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE/** Currently we are not aware of any exploits for these vulnerabilities.	IMLib/IMLib2 Multiple BMP Image Decoding Buffer Overflows CVE Names: CAN-2004-0817 CAN-2004-0802	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 1, 2004 Gentoo Linux Security Advisory, GLSA 200409-12, September 8, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:089, September 8, 2004 Fedora Update Notifications, FEDORA-2004-300 &301, September 9, 2004 Turbolinux Security Advisory, TLSA-2004-27, September 15, 2004 RedHat Security Advisory, RHSA-2004:465-08, September 15, 2004 Debian Security Advisories, DSA 547-1 & 548-1, September 16, 2004 Conectiva Linux Security Announcement, CLA-2004:870, September 28, 2004 Sun(sm) Alert Notifications, 57645 & 57648, September 20, 2004 Turbolinux Security Announcement, October 5, 2004 RedHat Security Update, RHSA-2004:480-05, October 20, 2004 Ubuntu Security Notice USN-35-1, November 30, 2004 RedHat Security Advisory, RHSA-2004:636-03, December 8, 2004 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**
Multiple Vendors Gentoo Linux; RedHat Fedora Core3, Core2; SUSE Linux 8.1, 8.2, 9.0-9.2, Desktop 1.0, Enterprise Server 9, 8, Novell Linux Desktop 1.0; X.org X11R6 6.7 .0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0-4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1 4.3 .0	Multiple vulnerabilities exist due to integer overflows, memory access errors, input validation errors, and logic errors, which could let a remote malicious user execute arbitrary code, obtain sensitive information or cause a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200411-28.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE X.org:	Multiple Vendors LibXPM Multiple Vulnerabilities CVE Name: CAN-2004-0914	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	X.Org Foundation Security Advisory, November 17, 2004 Fedora Update Notifications, FEDORA-2004-433 & 434, November 17 & 18, 2004 SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004 Gentoo Linux Security Advisory, GLSA 200411-28, November 19, 2004 Fedora Security Update Notifications FEDORA-2003-464, 465, 466, &

	http://www.x.org/pub/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-537.html Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:137 (libxpm) http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:138 (XFree86) Debian: http://www.debian.org/security/2004/dsa-607 (XFree86) SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ TurboLinux: http://www.turbolinux.com/update/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-023_RHSA-2004-537.pdf** **http://support.avaya.com/elmodocs2/security/ASA-2005-025_RHSA-2005-004.pdf** Currently we are not aware of any exploits for these vulnerabilities.			467, December 1, 2004 RedHat Security Advisory, RHSA-2004:537-17, December 2, 2004 Mandrakesoft: MDKSA-2004:137: libxpm4; MDKSA-2004:138: XFree86, November 22, 2004 Debian Security Advisory DSA-607-1 xfree86 -- several vulnerabilities, December 10, 2004 Turbolinux Security Announcement, January 20, 2005 **Avaya Security Advisories, ASA-2005-023 & 025, January 25, 2005**
Multiple Vendors Linux kernel 2.2-2.2.2.27 -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/ SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-016.html http://rhn.redhat.com/errata/RHSA-2005-017.html **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Exploit scripts have been published.	Linux Kernel Symmetrical Multiprocessing Page Fault Superuser Privileges CVE Name: CAN-2005-0001	High	SecurityTracker Alert, 1012862, January 12, 2005 SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005 RedHat Security Advisory, RHSA-2005:016-13 & 017-14, January 21, 2005 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 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,	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	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, November 19, 2004 SUSE Security Summary Report, SUSE-SR:2004:003, December 7, 2004 SecurityFocus, December 14, 2004 Fedora Update Notifications, FEDORA-2004-581 & 582, January 4, 2005 Avaya Security Advisory, ASA-2005-006, January 14, 2006

R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0	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 **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.			**Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
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/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Another exploit script has been published.**	Linux Kernel uselib() Root Privileges CVE Name: CAN-2004-1235	High	iSEC Security Research Advisory, January 7, 2005 Fedora Update Notifications, FEDORA-2005-013 & 014, January 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0001, January 13, 2005 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005** **PacketStorm, January 27, 2005**
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_3TUmq Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-043.html http://rhn.redhat.com/errata/RHSA-2005-017.html **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** 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 Secure Linux Security Advisory, TSLSA-2005-0001, January 13, 2005 RedHat Security Advisories, RHSA-2005:043-13 & RHSA-2005:017-14m January 18 & 21, 2005 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 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 **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** 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, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 Red Hat Advisory: RHSA-2004:549-10, December 2, 2004 RedHat Security Advisories, RHSA-2004:504-13 & 505-14, December 13, 2004 Avaya Security Advisory, ASA-2005-006, January 14, 2006 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.9; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32; SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9	Multiple remote Denial of Service vulnerabilities exist in the SMB filesystem (SMBFS) implementation due to various errors when handling server responses. This could also possibly lead to the execution of arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ 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 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities	Multiple Vendors smbfs Filesystem Memory Errors Remote Denial of Service CVE Names: CAN-2004-0883 CAN-2004-0949	Low/High (High if arbitrary code can be executed)	e-matters GmbH Security Advisory, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 Red Hat Advisory: RHSA-2004:549-10, December 2, 2004 Ubuntu Security Notice, USN-39-1, December 16, 2004 RedHat Security Advisories, RHSA-2004:504-13 & 505-14, December 13, 2004 SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005** **US-CERT Vulnerability Note, VU#726198, February 1, 2005**

Multiple Vendors Linux kernel 2.4-2.4.28	A vulnerability exists in the device drivers due to failure to implement all required virtual memory access flags. RedHat: http://rhn.redhat.com/errata/RHSA-2005-016.html http://rhn.redhat.com/errata/RHSA-2005-017.html Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Device Driver Virtual Memory Flags Implementation Failure CVE Name: CAN-2004-1057	Not Specified	RedHat Security Advisories, RHSA-2005:016-13 & 076-14, January 21, 2005
Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The Linux kernel /proc filesystem is susceptible to an information disclosure vulnerability. This issue is due to a race-condition allowing unauthorized access to potentially sensitive process information. This vulnerability may allow malicious local users to gain access to potentially sensitive environment variables in other users processes. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel PROC Filesystem Local Information Disclosure CVE Name: CAN-2004-1058	Medium	Ubuntu Security Notice USN-38-1 December 14, 2004 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The Linux kernel is prone to a local Denial of Service vulnerability. This vulnerability is reported to exist when 'CONFIG_SECURITY_NETWORK=y' and 'CONFIG_SECURITY_SELINUX=y' options are set in the Linux kernel. A local attacker may exploit this vulnerability to trigger a kernel panic and effectively deny service to legitimate users. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Sock_DGram_SendMsg Local Denial of Service CVE Name: CAN-2004-1069	Low	Ubuntu Security Notice USN-38-1 December 14, 2004 Fedora Update Notifications, FEDORA-2004-581 & 582, January 4, 2005 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
Multiple Vendors Linux kernel 2.6 -test1-test11, 2.6-l 2.6.8; SuSE Linux 9.1	A remote Denial of Service vulnerability exists in the iptables logging rules due to an integer underflow. Update available at: http://kernel.org/ SuSE: ftp://ftp.suse.com/pub/suse/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** A Proof of Concept exploit script has been published.	Linux Kernel IPTables Logging Rules Remote Denial of Service CVE Name: CAN-2004-0816	Low	SuSE Security Announcement, SUSE-SA:2004:037, October 20, 2004 Packetstorm, November 5, 2004 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
Multiple Vendors Linux kernel 2.6.8 rc1-rc3	A Denial of Service vulnerability exists in the 'ReiserFS' file system functionality due to a failure to properly handle files under certain conditions. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.9.tar.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.	Multiple Vendors Linux Kernel ReiserFS File System Local Denial of Service CVE Name: CAN-2004-0814	Low	SecurityFocus, October 26, 2004 Ubuntu Linux Security Advisory USN-38-1, December 14, 2004 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**

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/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** 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 Advisory, SA13308, November 25, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 SecurityFocus, December 16, 2004 Trustix Secure Linux Security Advisory, TSLSA-2005-0001, January 13, 2005 **Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005**
Multiple Vendors Samba Samba 2.2 a, 2.2 .0a, 2.2 .0, 2.2.1 a, 2.2.2, 2.2.3 a, 2.2.3-2.2.9, 2.2.11, 3.0, alpha, 3.0.1-3.0.5; MandrakeSoft Corporate Server 2.1, x86_64, 9.2, amd64	A vulnerability exists due to input validation errors in 'unix_convert()' and 'check_name()' when converting DOS path names to path names in the internal filesystem, which could let a remote malicious user obtain sensitive information. Samba: http://download.samba.org/samba/ftp/patches/security/ http://us1.samba.org/samba/ftp/old-versions/samba-2.2.12.tar.gz Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/s/samba/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-498.html SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57694-1&searchclause=** There is no exploit code required.	Samba Remote Arbitrary File Access CVE Name: CAN-2004-0815	Medium	iDEFENSE Security Advisory, September 30, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:104, October 1, 2004 Debian Security Advisory DSA 600-1, October 7, 2004 RedHat Security Advisory, RHSA-2004:498-04, October 1, 2004 SUSE Security Announcement, SUSE-SA:2004:035, October 5, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0051, October 1, 2004 **Sun(sm) Alert Notification, 57694, January 18, 2005**
Multiple Vendors Squid 2.x; Gentoo Linux;Ubuntu Linux 4.1 ppc, ia64, ia32;Ubuntu Linux 4.1 ppc, ia64, ia32; **Conectiva Linux 9.0, 10.0**	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 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/**	Squid NTLM fakeauth_auth Helper Remote Denial of Service **CVE Name:** **CAN-2005-0096**	Low	Secunia Advisory, SA13789, January 11, 2005 Gentoo Linux Security Advisor, GLSA 200501-25, January 17, 2005 Ubuntu Security Notice, USN-67-1, January 20, 2005 **Conectiva Linux Security Announcement, CLA-2005:923, January 26, 2005**

	Currently we are not aware of any exploits for this vulnerability.			
Open Group Open Motif 2.x, Motif 1.x; **Avaya CMS Server 8.0, 9.0, 11.0, CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing**	Multiple vulnerabilities have been reported in Motif and Open Motif, which potentially can be exploited by malicious people to compromise a vulnerable system. Updated versions of Open Motif and a patch are available. A commercial update will also be available for Motif 1.2.6 for users, who have a commercial version of Motif. http://www.ics.com/developers/index.php?cont=xpm_security_alert Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-537.html Gentoo: http://security.gentoo.org/glsa/glsa-200410-09.xml Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/x/xfree86/ TurboLinux: http://www.turbolinux.com/update/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-023_RHSA-2004-537.pdf** **http://support.avaya.com/elmodocs2/security/ASA-2005-025_RHSA-2005-004.pdf** Currently we are not aware of any exploits for these vulnerabilities.	Open Group Motif / Open Motif libXpm Vulnerabilities CVE Names: CAN-2004-0687 CAN-2004-0688	High	Integrated Computer Solutions Secunia Advisory ID: SA13353, December 2, 2004 RedHat Security Advisory: RHSA-2004:537-17, December 2, 2004 Turbolinux Security Announcement, January 20, 2005 **Avaya Security Advisories, ASA-2005-023 & 025, January 25, 2005**
Openswan Openswan 1.0.4-1.0.8, 2.1.1, 2.1.2, 2.1.4-2.1.6, 2.2	A buffer overflow vulnerability exists in the 'get_internal_addresses()' function when Openswan is compiled with the XAUTH and PAM options are enabled, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.openswan.org/code/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.	Openswan XAUTH/PAM Remote Buffer Overflow CVE Name: CAN-2005-0162	High	iDEFENSE Security Advisory, January 26, 2005 Fedora Update Notification, FEDORA-2005-082, January 28, 2005
Petr Vandrovec ncpfs prior to 2.2.6	Two vulnerabilities exist: a vulnerability exists in 'ncpfs-2.2.0.18/lib/ncplib.c' due to improper access control in the 'ncp_fopen_nwc()' function, which could let a malicious user obtain unauthorized access; and a buffer overflow vulnerability exists in 'ncpfs-2.2.5/sutil/ncplogin.c' due to insufficient validation of the 'opt_set_volume_after_parsing_all_options()' function, which could let a malicious user execute arbitrary code. Update available at: ftp://platan.vc.cvut.cz/pub/linux/ncpfs/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-44.xml An exploit script has been published.	Petr Vandrovec ncpfs Access Control & Buffer Overflow CVE Names: CAN-2005-0013 CAN-2005-0014	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID: 1013019, January 28, 2005

PHP Group Debian Slackware Fedora pp 4.3.7 and prior	Updates to fix multiple vulnerabilities with php4 which could allow remote code execution. Debian: Update to Debian GNU/Linux 3.0 alias woody at http://www.debian.org/releases/stable/ Slackware: http://www.slackware.com/security/viewer.php?l=slackware- security&y=2004&m=slackware-security.406480 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/ **Apple:** **http://www.apple.com/support/downloads/** An exploit script has been published.	PHP 'memory_limit' and strip_tags() Remote Vulnerabilities CVE Names: CAN-2004-0594 CAN-2004-0595	High	Secunia, SA12113 and SA12116, July 21, 2004 Debian, Slackware, and Fedora Security Advisories Turbolinux Security Advisory TLSA-2004-23, September 15, 2004 PacketStorm, December 11, 2004 **Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005**
PostgreSQL PostgreSQL 7.4.5; **Avaya CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0**	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/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-16.xml Debian: http://security.debian.org/pool/updates/main/p/postgresql/ OpenPKG: ftp://ftp.openpkg.org/release/ Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:149 Red Hat: http://rhn.redhat.com/errata/RHSA-2004-489.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-024_RHSA-2004-489.pdf** There is no exploit code required.	PostgreSQL Insecure Temporary File Creation CVE Name: CAN-2004-0977	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory, GLSA 200410-16, October 18, 2004 Debian Security Advisory, DSA 577-1, October 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.046, October 29, 2004 Mandrakesoft Security Advisory, MDKSA-2004:149, December 13, 2004 Red Hat Advisory RHSA-2004:489-17, December 20, 2004 **Avaya Security Advisory, ASA-2005-024, January 25, 2005**
Remote Sensing LibTIFF 3.5.7, 3.6.1, 3.7.0; **Avaya CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0**	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/RHSA-2005-019.html	Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities CVE Name: CAN-2004-1308	High	iDEFENSE Security Advisory 12.21.04 Secunia SA13629, December 23, 2004 SUSE Security Announcement, SUSE-SA:2005:001, January 10, 2005 RedHat Security Advisory, RHSA-2005:019-11, January 13, 2005 US-Cert Vulnerability Note, VU#125598, January 14, 2005 SGI Security Advisory, 20050101-01-U, January 19, 2005 Turbolinux Security Announcement, January 20, 2005 Conectiva Linux Security Announcement, CLA-2005:920, January 20, 2005 **Avaya Security Advisory, ASA-2005-021, January 25, 2005**

	SGI: http://support.sgi.com/browse_request/linux_patches_by_os TurboLinux: http://www.turbolinux.com/update/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-021_RHSA-2005-019.pdf** Currently we are not aware of any exploits for these vulnerabilities.			
rinetd rinetd 0.52, 0.61, 0.62	A buffer overflow vulnerability exists due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. No workaround or patch available at time of publishing. An exploit has been published but has not been released to the public.	RinetD select() Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bugtraq, January 24, 2005
SCO Open Server 5.0-5.0.7	A buffer overflow vulnerability exists in the scosession due to insufficient validation of user-supplied input strings prior to copying them to finite process buffers, which could let a malicious user execute arbitrary code. Updates available at: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.5 Currently we are not aware of any exploits for this vulnerability.	SCO scosession Buffer Overflow CVE Name: CAN-2003-1021	High	SCO Security Advisory, SCOSA-2005.5, January 26, 2005
splitbrain.org DokuWiki 2005-01-16 & prior	A vulnerability exists if 'userewrite' is enabled, which could let a remote malicious user obtain sensitive information. Update available at: http://www.splitbrain.org/Programming/PHP/DokuWiki/index.php A Proof of Concept exploit has been published.	DokuWiki 'userewrite' Mode Information Disclosure	Medium	SecurityTracker Alert, 1013035, January 28, 2005
Squid-cache.org Squid 2.5-STABLE6, 3.0-PRE3-20040702; when compiled with SNMP support	A remote Denial of Service vulnerability exists in the 'asn_parse_header()' function in 'snmplib/asn1.c' due to an input validation error when handling certain negative length fields. Updates available at: http://www.squid-cache.org/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-15.xml Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-591.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/s/squid/ OpenPKG: ftp://ftp.openpkg.org/release/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/**	Squid Remote Denial of Service CVE Name: CAN-2004-0918	Low	iDEFENSE Security Advisory, October 11, 2004 Fedora Update Notification, FEDORA-2004-338, October 13, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-15, October 18, 2004 RedHat Security Advisory, RHSA-2004:591-04, October 20, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:112, October 21, 2004 Debian Security Advisory, DSA 576-1, October 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.048, October 29, 2004 Conectiva Linux Security Announcement, CLA-2004:882, November 3, 2004 Ubuntu Security Notice, USN-19-1, November 6, 2004 **Conectiva Linux Security Announcement, CLA-2005:923, January 26, 2005**

	We are not aware of any exploits for this vulnerability.			
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; **Conectiva Linux 9.0, 10.0**	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 Debian: http://security.debian.org/pool/updates/main/s/squid/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit required.	Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow CVE Names: CAN-2005-0094 CAN-2005-0095	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA13825, January 13, 2005 Debian Security Advisory, DSA 651-1, January 20, 2005 Ubuntu Security Notice, USN-67-1, January 20, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:014, January 25, 2005 **Conectiva Linux Security Announcement, CLA-2005:923, January 26, 2005**
Sun Microsystems, Inc. Solaris 8.0 _x86, 8.0	A vulnerability exists in the 'dhcpconfig(1M),' 'pntadm(1M),' and 'dhcpmgr(1M)' DHCP administration utilities due to insufficient validation of the 'LD_LIBRARY_PATH' environment variable, which could let a malicious user execute arbitrary code with root privileges. Workaround available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57727-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris DHCP Utilities Arbitrary Code Execution	High	Sun(sm) Alert Notification, 57727, January 19, 2005
Sun Microsystems, Inc. Solaris 8.0 _x86, 8.0, 9.0 _x86, 9.0	A Denial of Service vulnerability exists due to a failure to handle excessive UDP endpoint activity. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1-21-117351-16-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris UDP Processing Denial of Service	Low	Sun(sm) Alert Notification, 57728, January 26, 2005
Threaded Read News trn 4.0	A buffer overflow vulnerability exists is due to improper validation of user-supplied string lengths, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Threaded Read News Buffer Overflow	High	SecurityFocus, January 27, 2005
University of Washington imap 2004b, 2004a, 2004, 2002b-2002e	A vulnerability exists due to a logic error in the Challenge-Response Authentication Mechanism with MD5 (CRAM-MD5) code, which could let a remote malicious user bypass authentication. Update available at: ftp://ftp.cac.washington.edu/mail/imap-2004b.tar.Z Currently we are not aware of any exploits for this vulnerability.	University Of Washington IMAP Server CRAM-MD5 Remote Authentication Bypass	Medium	US-CERT Vulnerability Note, VU#702777, January 27, 2005

X.org X11R6 6.7 .0, 6.8, 6.8.1	A vulnerability exists due to the insecure creation of socket directories, which could let a malicious user hijack socket sessions. Updates available at: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.8 Currently we are not aware of any exploits for this vulnerability.	X.org X Window Server Socket Hijacking CVE Name: CAN-2005-0134	Medium	SCO Security Advisory, SCOSA-2005.8, January 26, 2005
xmlsoft.org Libxml2 2.6.12-2.6.14	Multiple buffer overflow vulnerabilities exist: a vulnerability exists in the 'xmlNanoFTPScanURL()' function in 'nanoftp.c' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'xmlNanoFTPScanProxy()' function in 'nanoftp.c,' which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handling of DNS replies due to various boundary errors, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://xmlsoft.org/sources/libxml2-2.6.15.tar.gz OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-05.xml Mandrake: http://www.mandrakesoft.com/security/advisories OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: http://www.trustix.org/errata/2004/0055/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libx/libxml2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-615.html Conectiva: ftp://atualizacoes.conectiva.com.br/1 RedHat (libxml): http://rhn.redhat.com/errata/RHSA-2004-650.html **Apple:** **http://www.apple.com/support/downloads/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** An exploit script has been published.	xmlsoft.org Libxml2 Multiple Remote Stack Buffer Overflows CVE Name: CAN-2004-0989 CAN-2004-0110	High	SecurityTracker Alert I, 1011941, October 28, 2004 Fedora Update Notification, FEDORA-2004-353, November 2, 2004 Gentoo Linux Security Advisory, GLSA 200411-05, November 2,2004 Mandrakelinux Security Update Advisory, MDKSA-2004:127, November 4, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.050, November 1, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0055, November 1, 2004 Ubuntu Security Notice, USN-10-1, November 1, 2004 Red Hat Security Advisory, RHSA-2004:615-11, November 12, 2004 Conectiva Linux Security Announcement, CLA-2004:890, November 18, 2004 Red Hat Security Advisory, RHSA-2004:650-03, December 16, 2004 **Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005** **Turbolinux Security Advisory, TLSA-2005-11, January 26, 2005**
xtrlock xtrlock 2.0	A buffer overflow vulnerability exists due to insufficient boundary checks, which could let a malicious user cause a Denial of Service and take over the desktop session. Debian: http://security.debian.org/pool/updates/main/x/xtrlock/ Currently we are not aware of any exploits for this vulnerability.	xtrlock Buffer Overflow CVE Name: CAN-2005-0079	Low	Debian Security Advisory, DSA 649-1, January 20, 2005

Yukihiro Matsumoto Ruby 1.8.x	A remote Denial of Service vulnerability exists due to an input validation error in 'cgi.rb.' Debian: http://security.debian.org/pool/updates/main/r/ruby Mandrake: http://www.mandrakesoft.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/r/ruby1.8/l Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-23.xml Red Hat: http://rhn.redhat.com/errata/RHSA-2004-635.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-635.html **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Yukihiro Matsumoto Ruby Infinite Loop Remote Denial of Service CVE Name: CAN-2004-0983	Low	Secunia Advisory, SA13123, November 8, 2004 Ubuntu Security Notice, USN-20-1, November 9, 2004 Fedora Update Notification, FEDORA-2004-402 & 403, November 11 & 12, 2004 Gentoo Linux Security Advisory, GLSA 200411-23, November 16, 2004 Red Hat Advisory, RHSA-2004:635-03, December 13, 2004 RedHat Security Advisory, RHSA-2004:635-06, January 17, 2005 SGI Security Advisory, 20050101-01-U, January 19, 2005 **Turbolinux Security Announcement, 20050131, January 31, 2005**
zhcon zhcon 0.2-0.2.3	A vulnerability exists because a configuration file can be accessed with elevated privileges, which could let an unauthorized malicious user obtain sensitive information. Debian: http://security.debian.org/pool/updates/main/z/zhcon/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.	ZHCon Information Disclosure CVE Name: CAN-2005-0072	Medium	Debian Security Advisory DSA 655-1, January 25, 2005 Mandrake Security Advisory, MDKSA-2005:012, January 24, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
3proxy 3proxy 0.4	A buffer overflow vulnerability exists due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. Upgrade available at: http://www.security.nnov.ru/soft/3proxy/ An exploit has been published but has not been released to the public.	3proxy select() Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bugtraq, January 24, 2005
Aldoir Ventura UebiMiau prior to 2.7.2	A vulnerability exists that could let a remote malicious user access the 'database' directory to take control of user sessions and obtain user information. A fixed version (2.7.2) is available at: http://www.uebimiau.org/ A Proof of Concept exploit has been published.	Aldoir Ventura UebiMiau Data/File Disclosure	Medium	SecurityTracker Alert ID: 1013027, January 28, 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 **Gentoo: http://security.gentoo.org/glsa/glsa-200501-36.xml** An exploit script has been published.	AWStats Multiple Remote Input Validation	High	Securiteam, January 18, 2005 PacketStorm, January 25, 2005 **Gentoo Advisory: GLSA 200501-36 January 25, 2005**
Cisco Cisco devices running IOS and configured for IPv6	A remote Denial of Service vulnerability exists in the processing of IPv6 packets. The vendor has issued a solution at: http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco IOS IPv6 Packets Denial of Service CVE Name: CAN-2004-0467	Low	Cisco Security Advisory, 63844, January 26, 2005 Technical Cyber Security Alert, TA05-026A, January 26, 2005 US-CERT Vulnerability Note, VU#472582, January 26, 2005
Cisco Cisco devices running IOS enabled for BGP	A remote Denial of Service vulnerability exists if malformed BGP packets are submitted. The vendor has issued a solution at: http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco IOS BGP Packets Denial of Service	Low	Cisco Security Advisory 63845, January 29, 2005 Technical Cyber Security Alert, TA05-026A, January 26, 2005 US-CERT Vulnerability Note VU#689326, January 26, 2005
Cisco Cisco IOS 12.1T, 12.2, 12.2T, 12.3 and 12.3T	A remote Denial of Service vulnerability exists in the processing of Multi Protocol Label Switching (MPLS) packets. The vendor has issued a solution at: http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco IOS MPLS Packets Denial of Service	Low	Cisco Security Advisory 63846, January 28, 2005 Technical Cyber Security Alert, TA05-026A, January 26, 2005 US-CERT Vulnerability Note VU#583638, January 26, 2005
Comdev eCommerce 3.0	An input validation vulnerability could permit a remote malicious user to conduct Cross-Site Scripting attacks. The 'index.php' script does not properly validate user-supplied input in the start, category_id, keyword, pageaction and product_id parameters. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Comdev eCommerce Input Validation	High	SystemSecure, SS#24012005, January 26, 2005
GNU CitrusDB prior to 0.3.6	A vulnerability exists that could permit a remote malicious user to obtain credit card import and export data. The vendor has issued a fixed version (0.3.6), available at: http://www.citrusdb.org/download.php Currently we are not aware of any exploits for this vulnerability.	GNU CitrusDB Data Disclosure	Medium	OSVDB Reference: 13228, January 28, 2005
GNU Exponent CMS 0.95	Multiple vulnerabilities exist that could permit a remote malicious user to determine the installation path or conduct Cross-Site Scripting attacks. 'index.php' does not properly validate user-supplied input in the 'module' variable. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU Exponent CMS Cross-Site Scripting	High	Secunia SA13988, January 26, 2005
GNU MoinMoin 1.3.2	A vulnerability exists due to an unspecified error in the data retrieval of ACL protected pages in a search that could permit a user to bypass certain security restrictions. Update to version 1.3.3: http://sourceforge.net/project/showfiles.php?group_id=8482 Currently we are not aware of any exploits for this vulnerability.	MoinMoin Security Bypass	Medium	Secunia SA14001, January 26, 2005
GNU phpEventCalendar 0.2	A Cross-Site Scripting vulnerability exists because of improper input validation in the title and event text parameters. A remote malicious user access cookies, access data submitted through web forms, or take actions on the site acting as the target user. A fixed version (0.2.1) is available at: http://www.ikemcg.com/scripts/pec/downloads.html A patch for version 0.2 is available at: http://www.ikemcg.com/scripts/pec/downloads/pec-0.2-patch.tar.gz	GNU phpEventCalendar Input Validation	High	SecurityTracker Alert ID: 1012998, January 25, 2005

	A Proof of Concept exploit has been published.			
GNU Siteman 1.1.9	An authentication vulnerability exists that could permit a remote malicious user to gain administrative access by sending a special HTTP POST request to the 'users.php' script to add a user with administrative privileges. No workaround or patch available at time of publishing. **Another exploit script has been published.**	GNU Siteman Escalated Privilege	High	SecurityTracker Alert ID: 1012951, January 20, 2005 **PacketStorm, January 27, 2006**
GNU TikiWiki versions prior to 1.8.5 and 1.9 DR4	Multiple vulnerabilities exist due to missing validation of files placed in the 'temp' directory. This can be exploited to execute arbitrary PHP scripts. Update to version 1.8.5: http://sourceforge.net/project/showfiles.php?group_id=64258 **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200501-41.xml** Currently we are not aware of any exploits for these vulnerabilities.	GNU TikiWiki Remote Code Execution	High	TikiWiki January Security Alert, January 16, 2005 **Gentoo GLSA 200501-41 / tikiwiki, January 30, 2005**
GNU VooDoo cIRCle 1.x	A vulnerability exists due to an unspecified error related to the "NET_SEND" command affecting the Windows platform. Impact is unknown. Update to version 1.0.17 or later: http://sourceforge.net/project/showfiles.php?group_id=116847 Currently we are not aware of any exploits for this vulnerability.	GNU VooDoo cIRCle Unspecified Vulnerability	Not Specified	SecurityFocus Bugtraq ID 12393, January 28, 2005
GNU XOOPS Incontent Module	A vulnerability exists in the third party Incontent module that could permit a remote user to view the content of PHP files. The module does not properly validate user-supplied input in the 'url' parameter. A patch is available at: http://www.e-xoops.ru/modules/mydownloads/visit.php?lid=330 A Proof of Concept exploit has been published.	GNU XOOPS Incontent Module Information Disclosure	Medium	SecurityTracker Alert ID: 1013034, January 28, 2005
GPL ginp 0.20	A vulnerability exists that could permit users to bypass certain security restrictions. The is due to an error in the Java preferences API. Update to version 0.21: http://sourceforge.net/project/showfiles.php?group_id=105663 Currently we are not aware of any exploits for this vulnerability.	GPL ginp Security Restriction Bypass	Medium	SecurityFocus, Bugtraq ID 12386, January 27, 2005 Secunia, SA13993, January 27, 2005
GPL phpPgAds 2.x	An input validation vulnerability exists that could permit a Cross-Site Scripting attack. Input passed to the 'dest' parameter is not properly sanitized. Update to version 2.0.2: http://sourceforge.net/project/showfiles.php?group_id=36679 Currently we are not aware of any exploits for this vulnerability.	GPL phpPgAds 'dest' Parameter HTTP Response Splitting	High	Secunia, SA14051, January 28, 2005
Ingate Ingate Firewall 4.1.3 and prior	A vulnerability exists that permits a remote authenticated user with an active PPTP connection to the target firewall to remain connected after they have been disabled because the active PPTP connection remains active. No vendor upgrade is currently available. As a workaround, the vendor indicates that you can turn off the PPTP server and apply the configuration when you want to disable a PPTP user. Then, enable the PPTP server and re-apply the configuration. A Proof of Concept exploit has been published.	Ingate Firewall Disconnect Failure	Medium	SecurityTracker Alert ID, 1013022, January 28, 2005
James Seter BNC IRC proxy 2.8.4 and 2.9.2	A Denial of Service vulnerability exists due to a missing boundary check when doing 'FD_SET()' operations. This can be exploited to cause a buffer overflow. Update to version 2.9.3: http://www.gotbnc.com/download.html Currently we are not aware of any exploits for this vulnerability.	James Seter BNC IRC proxy Overflow	Low	Secunia SA14026, January 26, 2005
JShop E-Commerce JShop Server prior to 1.2.0	A vulnerability exists that could permit Cross-Site Scripting attacks. This is due to improper input validation in the 'xProd' and 'xSec' parameters in 'product.php.' Update to version 1.3.0: http://www.jshop.co.uk/ Currently we are not aware of any exploits for this vulnerability.	JShop Server Cross-Site Scripting	High	SystemSecure, SS#27012005, January 30, 2005
Juniper Networks All Juniper routers running JUNOS 5.x, JUNOS 6.x, JUNOS 7.x	A vulnerability exists that could permit a local or remote user to deliver certain packets to the router to cause a Denial of Service condition. Upgrades available to registered customers at: https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2005-01-010&actionBtn=Search	Juniper Networks JUNOS Software Denial of Service	Low	Juniper Security Bulletin PSN-2005-01-010 US-CERT Vulnerability Note VU#409555, January 26, 2005

	Currently we are not aware of any exploits for this vulnerability.			
Mozilla Bugzilla 2.x	**Incorrectly published under Windows Operating System section in Cyber Security Bulletin SB05-005.** A vulnerability exists which can be exploited by malicious people to conduct cross-site scripting attacks. Input passed in HTTP requests is not properly sanitized before being returned to users in error messages when an internal error is encountered. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Fixes are reportedly available in the CVS repository. Currently we are not aware of any exploits for this vulnerability.	Mozilla Bugzilla Internal Error	High	Bugzilla Bug 272620, January 3, 2005 Secunia SA13701, January 4, 2005
Mozilla Mozilla 0.x, 1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7.x Mozilla Firefox 0.x Mozilla Thunderbird 0.x	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird that can permit users to bypass certain security restrictions, conduct spoofing and script insertion attacks and disclose sensitive and system information. Mozilla: Update to version 1.7.5: http://www.mozilla.org/products/mozilla1.x/ Firefox: Update to version 1.0: http://www.mozilla.org/products/firefox/ Thunderbird: Update to version 1.0: http://www.mozilla.org/products/thunderbird/ Currently we are not aware of any exploits for these vulnerabilities.	Mozilla Firefox, Mozilla, and Thunderbird Multiple Vulnerabilities CVE Names: CAN-2005-0141 CAN-2005-0143 CAN-2005-0144 CAN-2005-0145 CAN-2005-0146 CAN-2005-0147 CAN-2005-0148 CAN-2005-0149 CAN-2005-0150	Medium/ High (High if arbitrary code can be executed)	Mozilla Foundation Security Advisory 2005-01, 03, 04, 07, 08, 09, 10, 11, 12
Mozilla Mozilla 1.7.3	A heap overflow vulnerability exists in the processing of NNTP URLs. A remote malicious user can execute arbitrary code on the target system. A remote user can create a specially crafted 'news://' URL that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The flaw resides in the *MSG_UnEscapeSearchUrl() function in 'nsNNTPProtocol.cpp'. The vendor has issued a fixed version (1.7.5), available at: http://www.mozilla.org/products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-03.xml SGI: http://support.sgi.com/browse_request/linux_patches_by_os **SuSE: ftp://ftp.suse.com/pub/suse/** A Proof of Concept exploit has been published.	Mozilla Buffer Overflow in Processing NNTP URLs	High	iSEC Security ResearchAdvisory, December 29, 2004 Gentoo Linux Security Advisor, GLSA 200501-03, January 5, 2005 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**
NEC socks5 1.0 r9	A buffer overflow vulnerability exists due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. No workaround or patch available at time of publishing. An exploit has been published but has not been released to the public.	NEC Socks5 select() Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bugtraq, January 24, 2005
Inferno Nettverk Dante 1.1	A buffer overflow vulnerability exists due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. No workaround or patch available at time of publishing. An exploit has been published but has not been released to the public.	Inferno Nettverk Dante select() Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bugtraq, January 24, 2005
Novell iChain 2.2, 2.3	A vulnerability exists that could allow a remote user to authenticate to iChain. If mutual authentication is enabled, authentication certificates are used on iChain accelerators, and multiple iChain environments are installed, then a remote user can authenticate to iChain using mutual authentication certificates. Refer to Novell advisory for solution: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10096315.htm Currently we are not aware of any exploits for this vulnerability.	Novell iChain Authentication	Medium	Novell TID10096315, January 25, 2005
OpenH323 OpenH323 Gatekeeper 2.0.9,	A buffer overflow vulnerability exists due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code.	OpenH323 select() Remote Buffer Overflow	Low/High (High if	Bugtraq, January 24, 2005

2.2	Upgrade available at: http://www.gnugk.org/h323download.html An exploit has been published but has not been released to the public.		arbitrary code can be executed)	
PEiD 0.x	A vulnerability exists due to a boundary error within the parsing of the PE (Portable Executable) import directory that could allow execution of arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	PEiD Buffer Overflow	High	iDEFENSE Security Advisory, January 24, 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 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/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-031.html SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ **Apple:** **http://www.apple.com/support/downloads/** There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHP Multiple Remote Vulnerabilities CVE Names: CAN-2004-1018 CAN-2004-1063 CAN-2004-1064 CAN-2004-1019 CAN-2004-1020 CAN-2004-1065	Medium/ High (High if arbitrary code can be executed)	Bugtraq, December 16, 2004 Conectiva Linux Security Announcement, CLA-2005:915, January 13, 2005 Red Hat, Advisory: RHSA-2005:031-08, January 19, 2005 SUSE Security Announcement, SUSE-SA:2005:002, January 17, 2005 Ubuntu Security Notice, USN-66-1, January 20, 2005 **Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005**
RealNetworks RealPlayer 10.5 and previous	A stack-based buffer overflow in the ShowPreferences method exists in the ActiveX control. This may permit a remote malicious user to execute arbitrary code on the user's system. Updates available: http://service.real.com/help/faq/security/040928_player/EN/ Currently we are not aware of any exploits for this vulnerability.	RealNetworks RealPlayer ActiveX Buffer Overflow	High	US-CERT Vulnerability Note, VU#698390, January 27, 2005
Squid-cache.org Squid 2.5	A vulnerability exists that could permit a remote malicious user to send multiple Content-length headers with special HTTP requests to corrupt the cache on the Squid server. A patch (squid-2.5.STABLE7-header_parsing.patch) is available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-header_parsing.patch Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000923 Currently we are not aware of any exploits for this vulnerability.	Squid Error in Parsing HTTP Headers CVE Name: CAN-2005-0175	Medium	SecurityTracker Alert ID, 1012992, January 25, 2005
SquirrelMail Development Team SquirrelMail 1.x	A Cross-Site Scripting vulnerability exists in the 'decodeHeader()' function in 'mime.php' when processing encoded text in headers due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://prdownloads.sourceforge.net/squirrelmail/sm143a-xss.diff?download Gentoo: http://security.gentoo.org/glsa/glsa-200411-25.xml	SquirrelMail Cross-Site Scripting CVE Name: CAN-2004-1036	High	Secunia Advisory, SA13155, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-25, November 17, 2004 Fedora Update Notifications,

	Conectiva: ftp://atualizacoes.conectiva.com.br/9 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Apple:** **http://www.apple.com/support/downloads/** **SuSE:** **ftp://ftp.suse.com/pub/suse/** An exploit script is not required.			FEDORA-2004-471 & 472, November 28, 2004 Conectiva Linux Security Announcement, CLA-2004:905, December 2, 2004 **Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005** **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**
Sun Microsystems, Inc. Sun Java JRE 1.3.x, 1.4.x, Sun Java SDK 1.3.x, 1.4.x; Conectiva Linux 10.0; Gentoo Linux; HP HP-UX B.11.23, B.11.22, B.11.11, B.11.00, HP Java SDK/RTE for HP-UX PA-RISC 1.3, HP Java SDK/RTE for HP-UX PA-RISC 1.4; Symantec Gateway Security 5400 Series v2.0.1, v2.0, Enterprise Firewall v8.0	A vulnerability exists due to a design error because untrusted applets for some private and restricted classes used internally can create and transfer objects, which could let a remote malicious user turn off the Java security manager and disable the sandbox restrictions for untrusted applets. Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1 Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-38.xml HP: http://www.hp.com/go/java Symantec: http://securityresponse.symantec.com/avcenter/security/Content/2005.01.04.html **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Sun Java Plug-in Sandbox Security Bypass CVE Name: CAN-2004-1029	Medium	Sun(sm) Alert Notification, 57591, November 22, 2004 US-CERT Vulnerability Note, VU#760344, November 23, 2004 Conectiva Linux Security Announcement, CLA-2004:900, November 26, 2004 Gentoo Linux Security Advisory, GLSA 200411-38, November 29, 2004 HP Security Bulletin, HPSBUX01100, December 1, 2004 Sun(sm) Alert Notification, 57591, January 6, 2005 (Updated) Symantec Security Response, SYM05-001, January 4, 2005 **SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005**
University of California (BSD License) PostgreSQL 7.x, 8.x	Multiple vulnerabilities exist that could permit malicious users to gain escalated privileges or execute arbitrary code. These vulnerabilities are due to an error in the 'LOAD' option, a missing permissions check, an error in 'contrib/intagg,' and a boundary error in the plpgsql cursor declaration. Update to version 8.0.1, 7.4.7, 7.3.9, or 7.2.7: http://wwwmaster.postgresql.org/download/mirrors-ftp Currently we are not aware of any exploits for these vulnerabilities.	University of California PostgreSQL Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	PostgreSQL Security Release, February 1, 2005
Xerox WorkCentre Pro 32 Color, 40 Color	A Directory Traversal vulnerability exists in the PostScript file interpretation code due to an input validation error, which could let a remote malicious user obtain sensitive information. Patch available at: http://www.xerox.com/downloads/usa/en/c/cert_XRX05_001_patch.zip There is no exploit code required.	Xerox WorkCenter Pro Directory Traversal	Medium	Secunia Advisory, SA13971, January 24, 2005

[back to top]

Recent Exploit Scripts/Techniques

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

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

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
February 1, 2005	ncpfsLocal.txt	Yes	Exploit for the Petr Vandrovec ncpfs Access Control & Buffer Overflow vulnerability.
February 1, 2005	xprallyboom.zip	Yes	Proof of Concept exploit for the Xpand Rally Remote Denial of Service vulnerability.
January 31, 2005	WC-ms05002-ani-expl-cb.c	Yes	Exploit for the Microsoft Windows ANI File Parsing Errors vulnerability
January 29, 2005	defeating-xpsp2-heap-protection.pdf	N/A	Analysis and code that defeats Microsoft Windows XP SP2 heap protection and data execution prevention mechanisms.
January 28, 2005	exploits-winamp.tgz	Yes	Exploits for the Nullsoft Winamp Variant IN_CDDA.dll Remote Buffer Overflow vulnerability.
January 28, 2005	NPPTNT2keylog.cpp	No	Proof of Concept exploit for the INCA nProtect Gameguard Unauthorized Read/Write Access vulnerability.
January 28, 2005	OutlookMuteX.txt	N/A	Exploit for Outlook that can press a button to verify it is okay to access protected contact data.
January 28, 2005	winamp_POC_M3U.txt	Yes	Proof of Concept exploit for the Nullsoft Winamp 'IN_CDDA.dll' Remote Buffer Overflow vulnerability.
January 27, 2005	cisco-torch.tar.bz2	N/A	Cisco Torch mass scanning, fingerprinting, and exploitation tool.
January 27, 2005	ex_gpsd.c	No	Script that exploits the Berlios GPSD Remote Format String vulnerability.
January 27, 2005	kbof_payload.txt	N/A	White paper discussing the smashing of the Linux kernel stack.
January 27, 2005	siteman.noam.txt	No	Exploit for the GNU Siteman Escalated Privilege vulnerability.
January 27, 2005	trn-test.txt trnBufferOverflowExpl.c	No	Exploits for the Threaded Read News Buffer Overflow vulnerability.
January 27, 2005	uselib24.c	Yes	Exploit for the Linux Kernel uselib() Root Privileges vulnerability.
January 27, 2005	WarFTPD_dos.pl	Yes	Proof of Concept exploit for the War FTP Daemon Remote Denial of Service vulnerability.
January 27, 2005	WIPv011.tgz	N/A	Whitepaper that gives an overview of a security assessment against Windows NT machines when penetration testing. Provides insight from both attacker and administrative perspectives.
January 25, 2005	w32dasmbof.disasm_me	No	Proof of Concept exploit for the W32Dasm Remote Buffer Overflow vulnerability.

[back to top]

Trends

- A three-year research project conducted by the security firm, NTA Monitor, concludes that nine out of 10 virtual private networks have exploitable vulnerabilities.For more information, see: "Nine out of 10 VPNs 'not secure'" located at: http://www.vnunet.com/news/1160912
- Pharming , DNS poisoning or domain hijacks that redirect users to 'dodgy' URLs, is a technique developed for tricking users into visiting bogus websites. It avoids coaxing users into responding to junk email. For more information, see " Phishing morphs into pharming" located at: http://www.theregister.co.uk/2005/01/31/pharming/
- Security Methods Inc. is warning customers of bogus “Microsoft Security Bulletins” that prompt recipients to download software with the potential to disable antivirus and similar protection controls. This bogus bulletins install spyware or remote-controlled software. For more information, see " New Phishing Scam Cloaked As Security Update, Warns Security Methods Inc" located at: http://namct.com/news/index.php?p=1713&more=1&c=1&tb=1&pb=1
- Plugging network holes before attackers can use them had become a burden on system administrators so they're putting up more barriers to stop intruders. For more information, see: "Patching up problems" located at: http://news.com.com/Patching+up+problems/2100-7347_3-5553945.html

[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	Zafi-B	Win32 Worm	Stable	June 2004
3	Zafi-D	Win32 Worm	Slight Increase	December 2004
4	Bagle-AA	Win32 Worm	Slight Decrease	April 2004
5	Sober-I	Win32 Worm	Decrease	November 2004

6	Bagle-AU	Win32 Worm	Stable	October 2004
7	Netsky-Z	Win32 Worm	Stable	April 2004
8	Bagle.BB	Win32 Worm	Stable	September 2004
9	Netsky-Q	Win32 Worm	Stable	March 2004
10	Netsky-B	Win32 Worm	Stable	February 2004

Table Updated February 1, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Viruses or Trojans Considered to be a High Level of Threat**

  - **.Rar files**: System administrators and service providers have begun seeing virus-infected messages with a new type of attachment hitting their mail servers: an .rar archive. While not as widely known as .zip, .rar files are similar to .zip files in that they are containers used to hold one or more compressed files. One recent .rar virus is disguised as a patch from Microsoft. Anti-virus vendors have acknowledged the presence of viruses delivered as .rar files and are working to develop tools to identify and eradicate the malware. For more information, refer to: http://www.eweek.com/article2/0,1759,1756636,00.asp
  - **Bagle**: Security firms are reporting on the emergence of new Bagle virus variants that are proliferating in the wild. There are likely two different variants that are new. Many security firms have raised the threat level for the variants from moderate to severe or critical, as more instances of the rapidly spreading worm are reported. The Bagle worm contains a Trojan backdoor that allows a remote user to execute arbitrary code on the infected PC. In addition to having its payload distributed via an e-mail attachment, the latest variants are also proliferating via peer-to-peer (P2P) applications. For more information, refer to http://www.internetnews.com/security/article.php/3465321
  - **MySQL worm**: A worm that takes advantage of administrators' poor password choices has started spreading among database systems. The malicious program, known as the "MySQL bot" or by the name of its executable code, SpoolCLL, infects computers running the Microsoft Windows operating system and open-source database known as MySQL. The worm gets initial access to a database machine by guessing the password of the system administrator, using common passwords. It then uses a flaw in MySQL to run bot software which then takes full control of the system. For more information, refer to: http://news.com.com/MySQL+worm+hits+Windows+systems/2100-7349_3-5553570.html?tag=nl

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
Backdoor.Hebolani		Trojan
Backdoor.Ranky.S		Win32 Worm
Backdoor.Sdbot.AM		Trojan
Backdoor.Sdbot.AN		Trojan
Backdoor.Sdbot.AO		Win32 Worm
BackDoor-CNC	Trojan-Dropper.Win32.Small.qj Trojan.MulDrop.1472 TROJ_SMALL.SI W32/Aler.A.worm	Trojan
Bagle.BL	Bagle.AY W32/Bagle.BL.worm	Win32 Worm
Bropia.C	IM-Worm.Win32.VB.c W32.Bropia.C W32/Bropia-C W32/Bropia.worm.e Win32.Bropia.C Win32/Bropia.159744!Worm WORM_BROPIA.D	Win32 Worm
Cisum.A	W32/Cisum.A.worm	Win32 Worm
Gaobot.CRP	W32/Gaobot.CRP.worm	Win32 Worm
Linux/BackDoor-Caca	Backdoor.Linux.Sckit.c Troj/Rootkit-R	Trojan
Locknut.A	Gavno.B SymbOS/Locknut.A Gavno.A	Symbian OS Worm
Nuke-Rhad	Nuker.Win32.Click.22 TR/Nuker.Click Troj/Click-23	Trojan
PWSteal.Bancos.N		Win32 Worm
PWSteal.Tarno.M	Trojan-Spy.Win32.Negett.b	Trojan
Sober.J	Email-Worm.Win32.Sober.j Email-Worm.Win32.VB.af W32.Sober.J@mm W32/Reblin W32/Reblin.A@mm	Win32 Worm

	W32/Sober-J W32/Sober.J@mm W32/Sober.k@MM WORM_SOBER.J	
StartPage-FX		Trojan
StartPage-FY		Trojan
SYMBOS_GAVNO.A		Symbian OS Worm
SYMBOS_GAVNO.B		Symbian OS Worm
Troj/Banito-E		Win32 Worm
Troj/Goldun-G		Win32 Worm
Troj/Vidlo-H	Trojan-Downloader.Win32.Vidlo.h	Win32 Worm
Trojan.Regger.A		Trojan
VBS.Gormlez@mm		Visual Basic Worm
W32.Cissi.W		Win32 Worm
W32.Gaobot.CEZ	Backdoor.Agobot.nq W32/Gaobot.worm.gen.t	Win32 Worm
W32.Mugly.G@mm		Win32 Worm
W32.Mugly.H@mm		Win32 Worm
W32.Mydoom.AO@mm		Win32 Worm
W32.Spybot.IVQ	Backdoor.Win32.Wootbot.al Backdoor.Win32.Wootbot.gen W32/Forbot-DY W32/Gaobot.CRP.worm W32/Sdbot.worm!166912 W32/Sdbot.worm.gen.j Win32.ForBot.LM WORM_WOOTBOT.FV	Win32 Worm
W32.Unfunner.A		Win32 Worm
W32/Agobot-PI	Backdoor.Win32.Agobot.jg	Win32 Worm
W32/Bagle.bj@MM	Bagle.AX Bagle.AY Bagle.BK Email-Worm.Win32.Bagle.ay I-Worm.Bagle.AY probably W32.Beagle.AY@mm W32.Beagle.AZ@mm W32/Bagle-Gen W32/Bagle.BK.worm W32/Bagle.bk@MM Win32.Bagle.AU Win32/Bagle.BE@mm Worm/Bagle.AX WORM_BAGLE.AZ	Win32 Worm
W32/Bagle-AY	Email-Worm.Win32.Bagle.ax W32/Bagle.bj@MM WORM_BAGLE.AY	Win32 Worm
W32/Bobax-F		Win32 Worm
W32/Bobax-G	WORM_BOBAX.G	Win32 Worm
W32/Codbot-A		Win32 Worm
W32/Forbot-DR	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Forbot-DV	Backdoor.Win32.Wootbot.ad	Win32 Worm
W32/Fungmush.worm.gen		Win32 Worm
W32/Mugly.i@MM		Win32 Worm
W32/MyDoom-AN	WORM_MYDOOM.C	Win32 Worm
W32/Patco-A	Trojan.Win32.VB.nd	Win32 Worm
W32/Rbot-AIX		Win32 Worm
W32/Rbot-UU	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.j	Win32 Worm
W32/Rbot-UW		Win32 Worm
W32/Sober-J	Email-Worm.Win32.Sober.j Reblin	Win32 Worm
W32/Wurmark-F	Email-Worm.Win32.Wurmark.g W32/Mugly.h@MM WORM_MUGLY.H	Win32 Worm
Win32.Bagle.AT	Email-Worm.Win32.Bagle.ax W32/Bagle.BB@mm W32/Bagle.bj@MM Win32/Bagle.19731!Worm	Win32 Worm
Win32.Blewfit.A	Trojan-Spy.Win32.Qukart.s Win32/Qukart.A!Trojan	Trojan

Win32.Bropia.B	IM-Worm.Win32.VB.c W32.Spybot.Worm W32/Bropia-C W32/Bropia.B W32/Bropia.worm.d Win32/Bropia.196608!Worm WORM_BROPIA.D	Win32 Worm
Win32.Dudrev.A	Downloader-TA	Win32 Worm
Win32.Mydoom.AL	Email-Worm.Win32.Mydoom.ah Email-Worm.Win32.Mydoom.ai I-Worm.Mydoom.gen MyDoom.AN W32.Mydoom.AN@mm W32/Mydoom W32/MyDoom-AN W32/Mydoom.AN@mm W32/Mydoom.AP@mm W32/Mydoom.av@MM Win32.Mydoom.AL Win32/Mydoom.AL!Worm WORM_MYDOOM.AN WORM_MYDOOM.C	Win32 Worm
Win32.Rbot.BMB	Backdoor.Win32.Rbot.fy W32/Gaobot.worm.gen.l Win32/Rbot.BMB!Worm	Win32 Worm
Win32.Rbot.BNE	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.y Win32/Spybot.162304!Worm	Win32 Worm
Wootbot.AL	Backdoor.Win32.Wootbot.al Backdoor.Win32.Wootbot.gen Backdoor.Wootbot.gen	Win32 Worm
WORM_AHKER.B	Email-Worm.Win32.Anker.a W32.Ahker.B@mm	Win32 Worm
WORM_BROPIA.D		Win32 Worm
WORM_MUGLY.I		Win32 Worm
WORM_OPOSSUM.A		Win32 Worm
WORM_RBOT.AKW		Win32 Worm
WORM_SDBOT.ALS		Win32 Worm

[back to top]

Last updated February 02, 2005