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.

Vulnerabilities

- Windows Operating Systems
  - asppress ACS Blog Cross-Site Scripting Vulnerability
  - Citrix MetaFrame Conferencing Manager Access Control Vulnerability
  - Code Ocean Ocean FTP Server Multiple Connections Denial of Service
  - FUN labs Games Denial of Service Vulnerability
  - GNU FileZilla Server Denial of Service Vulnerabilities
  - MailEnable Standard SMTP Format String Vulnerability
  - Massimiliano Montoro Cain Abel Buffer Overflow Causes Remote Code Execution
  - Microsoft Office InfoPath 2003 Information Disclosure Vulnerability
  - Microsoft Windows Local Denial Of Service Vulnerability
  - **Microsoft ASP.NET Canonicalization (Updated)**
  - Microsoft Windows EMF File Denial of Service Vulnerability
  - **Microsoft Windows License Logging Service Buffer Overflow (Updated)**
  - Notify Technology NotifyLink Enterprise Server Multiple Vulnerabilities
  - Oleh Yuschuk OllyDbg Error in Loading Causes Denial of Service Vulnerability
  - ThePoolClub iPool Information Disclosure Vulnerability
  - ThePoolClub iSnooker Information Disclosure Vulnerability
  - Webroot Software My Firewall Plus Arbitrary File Corruption Vulnerability
  - Woodstone Servers Alive Help Function Escalated Privilege Vulnerability
- UNIX / Linux Operating Systems
  - **Apache mod_ssl SSLCipherSuite Access Validation (Updated)**
  - Apple Mac OS X Multiple Vulnerabilities
  - **Carnegie Mellon Cyrus IMAP Server Off-by-one Overflow (Updated)**
  - **Carnegie Mellon University Cyrus IMAP Server Multiple Remote Buffer Overflows (Updated)**
  - **Cyrus SASL Buffer Overflow & Input Validation (Updated)**
  - **Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow (Updated)**
  - GNU Lysator LSH Remote Denial of Service
  - **GNU Xpdf Buffer Overflow in doImage() (Updated)**
  - **Grip CDDB Query Buffer Overflow (Updated)**
  - **Hiroyuki Yamamoto Sylpheed Mail Client Remote Buffer Overflow (Updated)**
  - **ImageMagick Remote EXIF Parsing Buffer Overflow (Updated)**
  - Initial Redirect Remote Buffer Overflow
  - **John Bradley XV File Name Handling Remote Format String (Updated)**
  - KDE DCOPServer Local Denial of Service
  - **KDE 'DCOPIDLING' Library (Updated)**
  - **Marc Lehmann rxvt-unicode 'command.c' Remote Buffer Overflow (Updated)**
  - **MIT Kerberos libkadm5srv Heap Overflow (Updated)**
  - **Mozilla Firefox Predictable Plugin Temporary Directory (Updated)**
  - Multiple BSD Vendor Copyout Kernel Memory Corrupt
  - **Multiple Vendors KPPP Privileged File Descriptor Information Disclosure (Updated)**
  - **Multiple Vendors Cyrus IMAPD Multiple Remote Vulnerabilities (Updated)**
  - **Multiple Vendors Cyrus IMAP 'imap magic plus' Buffer Overflow (Updated)**
  - **Multiple Vendors GNU Mailman Multiple Remote Vulnerabilities (Updated)**
  - **Multiple Vendors Perl 'rmtree()' Function Elevated Privileges (Updated)**
  - Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities
  - **Multiple Vendors nfs-utils 'SIGPIPE' TCP Connection Termination Denial of Service (Updated)**
  - **Multiple Vendors cURL / libcURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows (Updated)**
  - **Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows (Updated)**
  - **Multiple Vendors GNU Mailman Remote Directory Traversal (Updated)**
  - Multiple Vendors Lgames LTris Local Global High Score File Buffer Overflow
  - **Multiple Vendors Linux Kernel uselib() Root Privileges (Updated)**
  - Multiple Vendors Linux Kernel Netfilter Memory Leak Denial of Service
  - **Multiple Vendors Linux Kernel PPP Driver Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel SYS_EPoll_Wait Elevated Privileges (Updated)**
  - **Multiple Vendors Postfix IPv6 Security Bypass (Updated)**
  - **Multiple Vendors LibXPM Bitmap_unit Integer Overflow (Updated)**
  - **Multiple Vendors XLI Internal Buffer Management (Updated)**

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability

will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
asppress ACS Blog 0.8 - 1.1b	An input validation vulnerability has been reported that could let a remote malicious user conduct Cross-Site Scripting attacks. This is due to input validation errors in the 'search.asp' script in the 'search' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	asppress ACS Blog Cross-Site Scripting Vulnerability	High	Security Tracker Alert, 1013470, March 18, 2005
Citrix MetaFrame Conferencing Manager 3.0	A vulnerability has been reported that could let a remote malicious user obtain keyboard and mouse control of a conference. Hotfix MCM300W012 available: http://support.citrix.com/kb/entry.jspa?externalID=CTX105574 Currently we are not aware of any exploits for this vulnerability.	Citrix MetaFrame Conferencing Manager Access Control Vulnerability CAN-2005-0821	Low	Citrix Document ID CTX105574, February 24, 2005
Code Ocean Ocean FTP Server 1.0	A vulnerability has been reported due to a connection handling error which could let remote users cause a Denial of Service. Update to version 1.01: http://www.codeocean.com/oceanftpserver/index.html A Proof of Concept exploit script has been published.	Code Ocean Ocean FTP Server Multiple Connections Denial of Service	Low	Secunia SA14662, March 22, 2005
FUN Labs 4X4 Off-road Adventure III; Cabela's Big Game Hunter 2004 Season; Cabela's Big Game Hunter 2005; Cabela's Dangerous Hunts; Cabela's Deer Hunt 2005 Season; Revolution; Secret Service - In harm's Way; Shadow Force: Razor Unit; US Most Wanted: Nowhere To Hide	A vulnerability has been reported that could let a remote malicious user cause the game service to crash or to stop accepting packets. A remote user can send an empty UDP packet or a special join packet to cause these errors. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	FUN labs Games Denial of Service Vulnerability	Low	Security Tracker Alert, 1013492, March 21, 2005
GNU FileZilla Server prior to 0.9.6	Multiple vulnerabilities have been reported that could let a remote malicious user cause a Denial of Service. This is due to an error when attempting to access a file containing a reserved MS-DOS device name and an error in the transfer logic when using zlib compression. Update to version 0.9.6: http://sourceforge.net/project/showfiles.php?group_id=21558 There is no exploit code required.	GNU FileZilla Server Denial of Service Vulnerabilities	Low	Security Focus, 12865, March 22, 2005
MailEnable MailEnable Standard 1.8	A vulnerability has been reported that could let remote malicious users cause a Denial of Service or execute arbitrary code. This is due to a format string error when handling command arguments in the SMTP communication. No workaround or patch available at time of publishing. An exploit script has been published.	MailEnable Standard SMTP Format String Vulnerability CAN-2005-0804	High	Secunia SA14627, March 18, 2005
Massimiliano Montoro Cain Abel 2.65	Multiple vulnerabilities have been reported, one of which, could let a remote malicious user execute arbitrary code. This is due to boundary errors which could lead to buffer overflows in IKE-PSK sniffer filter and the HTTP sniffer filter. A fixed version (2.66) is available at: http://www.oxid.it/cain.html Currently we are not aware of any exploits for these vulnerabilities.	Massimiliano Montoro Cain Abel Buffer Overflow Causes Remote Code Execution	High	Secunia SA14630, March 18, 2005
Microsoft Office InfoPath 2003 SP1	A vulnerability has been reported that could let a remote malicious user obtain system information and authentication data from form template files. This is because private information may be included in the form template file when the administrator creates a form and adds a connection to the database table or to a web service. While there is no solution at this time, the vendor has issued a Knowledge Base article to describe security and privacy considerations for creating forms: http://support.microsoft.com/kb/867443/ Currently we are not aware of any exploits for this vulnerability.	Microsoft Office InfoPath 2003 Information Disclosure Vulnerability CAN-2005-0820	Medium	Microsoft Knowledge Base 867443, February 22, 2005

Microsoft Windows XP Home SP1 Windows XP Media Center Edition SP1 Windows XP Professional SP1 Windows XP Tablet PC Edition SP1	A vulnerability has been reported that could permit a local malicious user to cause a Denial of Service. This is caused when a raw IP over IP socket is created and data is transferred over the newly created socket. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows Local Denial Of Service Vulnerability	Low	Security Focus, 12870, March 22, 2005
Microsoft ASP.NET 1.x	A vulnerability exists which can be exploited by malicious people to bypass certain security restrictions. The vulnerability is caused due to a canonicalization error within the .NET authentication schema. Apply ASP.NET ValidatePath module: http://www.microsoft.com/downloads/details.aspx?FamilyId=DA77B852-DFA0-4631-AAF9-8BCC6C743026 Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-004.mspx V1.1: Bulletin updated to include Knowledge Base Article numbers for each individual download under Affected Products. **V1.2: Bulletin "Caveats" section has been updated to document known issues that customers may experience when installing the available security updates.** A Proof of Concept exploit has been published.	Microsoft ASP.NET Canonicalization CVE Name: CAN-2004-0847	Medium	Microsoft, October 7, 2004 Microsoft Security Bulletin, MS05-004, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT VU#283646 Microsoft Security Bulletin, MS05-004 V1.1, February 15, 2005 **Microsoft Security Bulletin, MS05-004 V1.2, March 16, 2005**
Microsoft Microsoft Windows 2000 Advanced Server Microsoft Windows 2000 Datacenter Server Microsoft Windows 2000 Professional Microsoft Windows 2000 Server	A vulnerability has been reported that could let remote malicious users cause a Denial of Service. This is due to an error when processing EMF (Microsoft Enhanced Metafile) files in the 'GetEnhMetaFilePaletteEntries()' API in 'GDI32.DLL.' No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows EMF File Denial of Service Vulnerability CAN-2005-0803	Low	Secunia SA14631, March 18, 2005
Microsoft Windows NT Server 4.0 SP6a, Windows NT Server 4.0 Terminal Server Edition SP6a, Windows 2000 Server SP3 & SP4, Windows 2003, Windows 2003 for Itanium-based Systems **Windows Advanced Server SP4**	A buffer overflow vulnerability exists in the License Logging service due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-010.mspx V1.1: Bulletin updated to reflect a revised “Security Update Information” section for Windows Server 2003 **Windows 2000 Advanced Server vulnerable if Service Pack 4 not installed separately.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows License Logging Service Buffer Overflow CAN-2005-0050	Low/High (High if arbitrary code can be executed)	Microsoft Security Bulletin, MS05-010, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT VU#130433 Microsoft Security Bulletin, MS05-010 V1.1, February 23, 2005 **Immunity, Inc. Advisory, March 16, 2005**
Notify Technology NotifyLink Enterprise Server	Multiple vulnerabilities have been reported that could let a remote malicious user obtain sensitive information, bypass certain security restrictions, and conduct SQL injection attacks. These vulnerabilities are caused because administrative users can view other users' private credentials or disable functions for users via the web interface but functions are still accessible via the URL. Also, certain input is not properly validated before being used in an SQL query and AES keys can be obtained by submitting a special POST request. Update to version 3.0 or later and configure NotifyLink to use "Manual Key Generation". There is no exploit code required.	Notify Technology NotifyLink Enterprise Server Multiple Vulnerabilities CAN-2005-0809 CAN-2005-0810 CAN-2005-0811 CAN-2005-0812	High	Secunia SA14617, March 18, 2005 US-CERT VU#770532 US-CERT VU#131828 US-CERT VU#264097 US-CERT VU#581068

Oleh Yuschuk OllyDbg 1.10 and prior	A vulnerability has been reported in OllyDbg that could let a remote malicious user cause a Denial of Service. This is due to a flaw when loading a special DLL filename as a process. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Oleh Yuschuk OllyDbg Error in Loading Causes Denial of Service Vulnerability	Low	Security Focus,12850, March 19, 2005
ThePoolClub iPool 1.6.81 and prior	A vulnerability has been reported that could let a local malicious user obtain passwords. This is because the software stores user passwords in clear text in the 'Program Files\ThePoolClub\iPool\MyDetails.txt' file. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ThePoolClub iPool Information Disclosure Vulnerability CAN-2005-0823	Medium	Security Tracker Alert, 1013458 Date: March 16 2005
ThePoolClub iSnooker 1.6.81 and prior	A vulnerability has been reported that could let a local malicious user obtain passwords. This is because the software stores user passwords in clear text in the 'Program Files\TheSnookerClub\iSnooker\ MyDetails.txt' file. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ThePoolClub iSnooker Information Disclosure Vulnerability CAN-2005-0823	Medium	Security Tracker Alert, 1013459, March 16, 2005
Webroot Software My Firewall Plus 5.0 (build 1117)	A vulnerability has been reported that could let local malicious users change the content of arbitrary files. This is because the Log Viewer's export functionality saves log files without first dropping its privileges. Update to version 5.0 (build 1119) or apply patch: http://www.webroot.com/services/mfp_patch.exe Currently we are not aware of any exploits for this vulnerability.	Webroot Software My Firewall Plus Arbitrary File Corruption Vulnerability CAN-2005-0515	Medium	Secunia SA13577, March 18, 2005
Woodstone bvba Servers Alive 4.1, 5.0	A vulnerability has been reported in the Help function that could let a local malicious user can gain system privileges and execute arbitrary files. This is because a local user can open a help file in Notepad with system privileges. The user can then open 'cmd.exe.' No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Woodstone Servers Alive Help Function Escalated Privilege Vulnerability CAN-2005-0352	High	Security Focus, 12822, March 16, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source

Apache Software Foundation Apache 2.0.35-2.0.52	A vulnerability exists when the 'SSLCipherSuite' directive is used in a directory or location context to require a restricted set of cipher suites, which could let a remote malicious user bypass security policies and obtain sensitive information. OpenPKG: ftp://ftp.openpkg.org/release/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-21.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesoft.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-562.html SuSE: In the process of releasing packages. RedHat: http://rhn.redhat.com/errata/RHSA-2004-600.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-010_RHSA-2004-600.pdf VMware: http://www.vmware.com/download/esx/ **HP:** **http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01123** There is no exploit code required.	Apache mod_ssl SSLCipherSuite Access Validation CAN-2004-0885	Medium	OpenPKG Security Advisory, OpenPKG-SA-2004.044, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-21, October 22, 2004 Slackware Security Advisory, SSA:2004-299-01, October 26, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:122, November 2, 2004 Conectiva Linux Security Announcement, CLA-2004:885, November 4, 2004 Fedora Update Notification, FEDORA-2004-420, November 12, 2004 RedHat Security Advisory, RHSA-2004:562-11, November 12, 2004 SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004 RedHat Security Advisory, RHSA-2004:600-12, December 13, 2004 Avaya Security Advisory, ASA-2005-010, January 14, 2005 WMware Advisory, January 14, 2005 **HP Security Advisory, HPSBUX01123 , March 22, 2005**
Apple Mac OS X 10.3-10.3.8, Mac OS X Server 10.3-10.3.8	Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported due to a memory access error on the AFP server; a vulnerability has been reported in the permission settings in the directories used by the installer's receipt cache and system-level ColorSync profiles because they are configured with world-writable permissions, which could let a malicious user obtain elevated privileges; a vulnerability has been reported in the Bluetooth Setup Assistant application which could let a remote malicious user bypass security restrictions; a vulnerability has been reported due to insufficient validation of file permissions when accessing Drop Boxes, which could let a remote malicious user obtain sensitive information; and a buffer overflow vulnerability has been reported when handling 'CF_CHARSET_PATH' environment variables in the Core Foundation library, which could let a malicious user execute arbitrary code. Updates available at: http://www.apple.com/support/downloads/securityupdate2005003client.html An exploit script has been published.	Apple Mac OS X Multiple Vulnerabilities CAN-2005-0340 CAN-2005-0712 CAN-2005-0713 CAN-2005-0715 CAN-2005-0716	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	Apple Security Update, APPLE-SA-2005-03-21, March 21, 2005

Carnegie Mellon University Cyrus IMAP Server 2.2.9 and prior versions	A vulnerability exists in the mysasl_canon_user() function that could allow a remote user to execute arbitrary code on the target system. An off-by-one error exists in the mysasl_canon_user() function that may result in an unterminated user name string. A remote user may be able to trigger the buffer overflow to execute arbitrary code on the target system with the privileges of the target IMAP process. The vendor has issued a fixed version (2.2.10), available at: ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/ **Apple:** **http://www.apple.com/support/downloads/securityupdate2005003client.html** Currently we are not aware of any exploits for this vulnerability.	Carnegie Mellon Cyrus IMAP Server Off-by-one Overflow CAN-2004-1067	High	SecurityTracker Alert ID: 1012474, December 10, 2004 **Apple Security Update, APPLE-SA-2005-03-21, March 21, 2005**
Carnegie Mellon University Cyrus IMAP Server 2.x	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in mailbox handling due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the imapd annotate extension due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'fetchnews,' which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exist because remote administrative users can exploit the backend; and a buffer overflow vulnerability exists in imapd due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imapd-2.2.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200502-29.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Cyrus IMAP Server Multiple Remote Buffer Overflows CAN-2005-0546	High	Secunia Advisory, SA14383, February 24, 2005 Gentoo Linux Security Advisory, GLSA 200502-29, February 23, 2005 SUSE Security Announcement, SUSE-SA:2005:009, February 24, 2005 Ubuntu Security Notice USN-87-1, February 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:051, March 4, 2005 Conectiva Linux Security Announcement, CLA-2005:937, March 17, 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 FedoraLegacy: http://download.fedoralegacy.org/redhat/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Apple:** **http://www.apple.com/support/downloads/securityupdate2005003client.html** Currently we are not aware of any exploits for these vulnerabilities.	Cyrus SASL Buffer Overflow & Input Validation CAN-2004-0884 CAN-2005-0373	High	Security Tracker 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 Fedora Legacy Update Advisory, FLSA:2137, February 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005 SUSE Security Announcement, SUSE-SA:2005:013, March 3, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:054, March 16, 2005** **Apple Security Update, APPLE-SA-2005-03-21, March 21, 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:	Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow 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 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 SGI Security Advisory, 20050202-01-U, February 9, 2005 Gentoo Linux Security Advisory, GLSA 200502-10, February 9, 2005 Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003,

	http://security.ubuntu.com/ubuntu/pool/main/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE: ftp://ftp.suse.com/pub/suse/** FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-10.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ Trustix: http://http.trustix.org/pub/trustix/updates/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-026.html** Currently we are not aware of any exploits for this vulnerability.			February 11, 2005 Fedora Legacy Update Advisory, FLSA:2127, March 2, 2005 SUSE Security Announcement, SUSE-SA:2005:015, March 14, 2005 **RedHat Security Advisory, RHSA-2005:026-15, March 16, 2005** **SuSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005**
GNU Lysator LSH 1.5-1.5.5, 2.0	A remote Denial of Service vulnerability has been reported due to an unspecified error. Upgrades available at: http://www.lysator.liu.se/~nisse/archive/ Patch available at: ftp://ftp.lysator.liu.se/pub/security/lsh/lsh-2.0-2.0.1.diff.gz Currently we are not aware of any exploits for this vulnerability.	Lysator LSH Remote Denial of Service CAN-2005-0814	Low	Secunia Advisory, SA14609, March 17, 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):	GNU Xpdf Buffer Overflow in doImage() 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 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005

	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: 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/** FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-026.html** Currently we are not aware of any exploits for this vulnerability.			SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005 Fedora Legacy Update Advisory, FLSA:2127, March 2, 2005 SUSE Security Announcement, SUSE-SA:2005:015, March 14, 2005 **RedHat Security Advisory, RHSA-2005:026-15, March 16, 2005** **SuSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005**
Grip Grip 3.1.2, 3.2 .0	A buffer overflow vulnerability has been reported in the CDDB protocol due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates **Gentoo:**	Grip CDDB Query Buffer Overflow CAN-2005-0706	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005-202 & 203, March 9, 2005 **Gentoo Linux Security Advisory, GLSA 200503-21, March 17, 2005**

	http://security.gentoo.org/glsa/glsa-200503-21.xml Currently we are not aware of any exploits for this vulnerability.			
Hiroyuki Yamamoto Sylpheed 0.8.11, 0.9.4-0.9.12, 0.9.99, 1.0 .0-1.0.2	A buffer overflow vulnerability exists in certain headers that contain non-ASCII characters, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.3.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-303.html** **Gentoo: http://security.gentoo.org/glsa/glsa-200503-26.xml** Currently we are not aware of any exploits for this vulnerability.	Sylpheed Mail Client Remote Buffer Overflow CAN-2005-0667	High	Security Tracker Alert, 1013376, March 4, 2005 Fedora Update Notification, FEDORA-2005-211, March 15, 2005 **RedHat Security Advisory, RHSA-2005:303-05, March 18, 2005** **Gentoo Linux Security Advisory, GLSA 200503-26, March 20, 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.) http://rhn.redhat.com/errata/RHSA-2004-480.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for this vulnerability.	ImageMagick Remote EXIF Parsing Buffer Overflow CAN-2004-0827 CAN-2004-0981	High	Security Tracker 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, TLSA-2005-7, January 26, 2005 **Fedora Update Notification, FEDORA-2005-221, March 15, 2005**
Initial Redirect Squid Proxy Plug-In 0.1, 0.2	A buffer overflow vulnerability has been reported due to a failure to copy user-supplied data securely, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Upgrades available at: http://www.vanheusden.com/ir/ir-0.3.tgz Currently we are not aware of any exploits for	Initial Redirect Remote Buffer Overflow CAN-2005-0813	Low/ High (High if arbitrary code can be executed)	Security Focus, 12827, March 17, 2005

	this vulnerability.			
John Bradley XV 3.10 a	A format string vulnerability exists in a formatted printing function due to insufficient sanitization of user-supplied input, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-09.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	XV File Name Handling Remote Format String CAN-2005-0665	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200503-09, March 4, 2005 **SUSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005**
KDE KDE 1.1-1.1.2, 1.2, 2.1-2.1.2, 2.2-2.2.2, 3.0- 3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2	A Denial of Service vulnerability has been reported in the Desktop Communication Protocol (DCOP) daemon due to an error in the authentication process Upgrade available at: http://www.kde.org/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-22.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.	KDE DCOPServer Local Denial of Service CAN-2005-0396	Low	KDE Security Advisory, March 16, 2005
KDE kdelibs 3.3.2	A vulnerability exists in the 'dcopidling' library due to insufficient validation of a files existence, which could let a malicious user corrupt arbitrary files. Patch available at: http://bugs.kde.org/attachment.cgi?id=9205&action=view **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Gentoo: http://security.gentoo.org/glsa/glsa-200503-14.xml Currently we are not aware of any exploits for this vulnerability.	KDE 'DCOPIDLING' Library CAN-2005-0365	Medium	Security Focus, February 11, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:045, February 18, 2005 Gentoo Linux Security Advisory, GLSA 200503-14, March 7, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:058, March 16, 2005**
Marc Lehmann rxvt-unicode prior to 5.3	A buffer overflow vulnerability has been reported in 'command.c,' which could let a remote malicious user execute arbitrary code. Update available at: http://dist.schmorp.de/rxvt-unicode/rxvt-unicode-5.3.tar.bz2 **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-23.xml** Currently we are not aware of any exploits for this vulnerability.	Marc Lehmann rxvt-unicode 'command.c' Remote Buffer Overflow **CAN-2005-0764**	High	Secunia Advisory: SA14562, March 15, 2005 **Gentoo Linux Security Advisory, GLSA 200503-23, March 20, 2005**
MIT Kerberos 5 krb5-1.3.5 & prior; Avaya S8700/S8500/S8300 (CM2.0 and later), MN100, Intuity LX 1.1- 5.x, Modular Messaging MSS	A buffer overflow exists in the libkadm5srv administration library. A remote malicious user may be able to execute arbitrary code on an affected Key Distribution Center (KDC) host. There is a heap overflow in the password history handling code. A patch is available at: http://web.mit.edu/kerberos/advisories/2004-004-patch_1.3.5.txt Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-05.xml Debian: http://security.debian.org/pool/	Kerberos libkadm5srv Heap Overflow CAN-2004-1189	High	SecurityTracker Alert ID, 1012640, December 20, 2004 Gentoo GLSA 200501-05, January 5, 2005 Ubuntu Security Notice, USN-58-1, January 10, 2005 Conectiva Linux Security Announcement, CLA-2005:917, January 13, 2005 Avaya Security Advisory, ASA-2005-036, February 7, 2005 Sun(sm) Alert Notification,

	updates/main/k/krb5/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/k/krb5/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-036_RHSA-2005-012.pdf Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57712-1 **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.			57712, February 25, 2005 **Turbolinux Security Advisory, TLSA-2005-34, March 17, 2005**
Mozilla.org Firefox 1.0	A vulnerability exists because a predictable name issued for the plugin temporary directory, which could let a malicious user cause a Denial of Service or modify system/user information. Update available at: http://www.mozilla.org/products/firefox/all.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-10.xml **SuSE:** **ftp://ftp.suse.com/pub/suse/** An exploit has been published.	Mozilla Firefox Predictable Plugin Temporary Directory CAN-2005-0578	Low/Medium (Medium if user/system information can be modified)	Mozilla Foundation Security Advisory, 2005-28, February 25, 2005 **SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005**
Multiple BSD Vendors FreeBSD 4.10-PRERELEASE, 1.1.5 .1, 2.0, 2.0.5, 2.1 x, 2.1, 2.1.5-2.1.7 .1, 2.2 x, 2.2, 2.2.2-2.2.6, 2.2.8, 3.0 -RELENG, 3.0, 3.1 x, 3.1, 3.2 x, 3.2, 3.3 x, 3.3, 3.4 x, 3.4, 3.5 x, 3.5 -STABLEpre122300, 3.5 -STABLEpre050201, 3.5 -STABLE, 3.5, 3.5.1 -STABLEpre2001-07-20, 3.5.1 -STABLE, 3.5.1 -RELEASE, 3.5.1, 4..x, 4.0 -RELENG, 4.0 alpha, 4.0, 4.1, 4.1.1 -STABLE, 4.1.1 -RELEASE, 4.1.1, 4.2 -STABLEpre122300, 4.2 -STABLEpre050201, 4.2 -STABLE, 4.2 -RELEASE, 4.2, 4.3 -STABLE, 4.3 -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, 4.4 -RELENG, 4.4 -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, 4.5 -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, 4.6 -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 5.0 -RELENG,	A vulnerability has been reported in the 'copyout()' function due to insufficient sanitization of the destination argument, which could let a remote malicious user corrupt kernel memory. OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/i386/028_locore.patch Currently we are not aware of any exploits for this vulnerability.	Multiple BSD Vendor Copyout Kernel Memory Corrupt CAN-2005-0637	Medium	Security Focus, 12825, March 16, 2005

5.0 -RELEASE-p14, 5.0 alpha, 5.0, 5.1 -RELENG, 5.1 -RELEASE/Alpha, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3; NetBSD 1.0, 1.1, 1.2, 1.2.1, 1.3-1.3.3, 1.4 , x86, SPARC, arm32, Alpha, 1.4.1, x86, SPARC, sh3, arm32, Alpha, 1.4.2, x86, SPARC, arm32, Alpha, 1.4.3, 1.5, x86, sh3, 1.5.1-1.5.3, 1.6, beta, 1.6.1, 1.6.2, 2.0; OpenBSD 2.0-2.9, 3.0-3.6				
Multiple Vendors Bernd Johanness Wueb kppp 1.1.3; KDE KDE 1.1-1.1.2, 1.2, 2.0 BETA, 2.0-2.2.2, 3.0-3.0.5, 3.1-3.1.5, KDE KPPP 2.1.2	A vulnerability exists due to a file descriptor leak, which could let a malicious user obtain sensitive information. Patch available at: ftp://ftp.kde.org/pub/kde/security_patches RedHat: http://rhn.redhat.com/errata/RHSA-2005-175.html Debian: http://security.debian.org/pool/updates/main/k/kdenetwork/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.	KPPP Privileged File Descriptor Information Disclosure CAN-2005-0205	Medium	iDEFENSE Security Advisory, February 28, 2005 RedHat Security Advisory, RHSA-2005:175-06, March 3, 2005 Debian Security Advisory, DSA 692-1, March 8, 2005 **Conectiva Linux Security Announcement, CLSA-2005:934, March 16, 2005**

Multiple Vendors Carnegie Mellon University Cyrus IMAP Server 2.1.7, 2.1.9, 2.1.10, 2.1.16, 2.2 .0 ALPHA, 2.2.1 BETA, 2.2.2 BETA, 2.2.3-2.2.8; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PROXY' and 'LOGIN' commands if the 'IMAPMAGICPLUS' option is enabled, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists in the argument parser for the 'PARTIAL' command, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists in the argument handler for the 'FETCH' command, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handler for the 'APPEND' command, which could let a remote malicious user execute arbitrary code. Carnegie Mellon University: ftp://ftp.andrew.cmu.edu/pub/cyrus/ Debian: http://security.debian.org/pool/updates/main/c/cyrus-imapd/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-34.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ OpenPKG: ftp://ftp.openpkg.org/release/ SUSE: ftp://ftp.SUSE.com/pub/SUSE/ **Apple: http://www.apple.com/support/downloads/securityupdate2005003client.html** Currently we are not aware of any exploits for these vulnerabilities.	Cyrus IMAPD Multiple Remote Vulnerabilities CAN-2004-1011 CAN-2004-1012 CAN-2004-1013	High	Securiteam, November 23, 2004 Debian Security Advisory, DSA 597-1, November 25, 2004 Gentoo Linux Security Advisory, GLSA 200411-34, November 25, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:139, November 26, 2004 Trustix Secure Linux Advisory, TSL-2004-0063. November 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.051, November 29, 2004 Conectiva Linux Security Announcement, CLA-2004:904, December 1, 2004 Fedora Update Notifications, FEDORA-2004-487 & 489, December 1, 2004 SUSE Security Announcement, SUSE-SA:2004:043, December 3, 2004 **Apple Security Update, APPLE-SA-2005-03-21, March 21, 2005**
Multiple Vendors Carnegie Mellon University Cyrus IMAP Server 2.2.9 & prior	A buffer overflow vulnerability exists in the 'imap magic plus' support code, which could let a remote malicious user execute arbitrary code. Update available at: http://asg.web.cmu.edu/cyrus/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-34.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Conectiva:	Multiple Vendors Cyrus IMAP 'imap magic plus' Buffer Overflow CAN-2004-1015	High	Gentoo Linux Security Advisory, GLSA 200411-34, November 25, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:139, November 26, 2004 Secunia SA13349, December 2, 2004 Secunia Advisory ID: SA13346, December 2, 2004 Secunia Advisory ID: 13366, December 6, 2004 **Apple Security Update, APPLE-SA-2005-03-21, March 21, 2005**

	http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000904 SUSE: ftp.SUSE.com/pub/SUSE **Apple:** **http://www.apple.com/support/downloads/securityupdate2005003client.html** Currently we are not aware of any exploits for this vulnerability.			
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 Debian: http://security.debian.org/pool/updates/main/m/mailman/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-235.html** Currently we are not aware of any exploits for these vulnerabilities.	GNU Mailman Multiple Remote Vulnerabilities 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 Debian Security Advisories, DSA 674-1 & 674-2, February 10 & 11, 2005 SUSE Security Announcement, SUSE-SA:2005:007, February 14, 2005 Debian Security Advisory, DSA 674-3, February 21, 2005 **RedHat Security Advisory, RHSA-2005:235-05, March 21, 2005**
Multiple Vendors Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6	A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml **Debian:** **http://security.debian.org/pool/updates/main/p/perl/** Currently we are not aware of any exploits for this vulnerability.	Perl 'rmtree()' Function Elevated Privileges CAN-2005-0448	Medium	Ubuntu Security Notice, USN-94-1 March 09, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 **Debian Security Advisory, DSA 696-1 , March 22, 2005**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11	Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities CAN-2005-0815	High	Security Focus, 12837, March 18, 2005

Multiple Vendors nfs-utils 1.0.6	A vulnerability exists due to an error in the NFS statd server in 'statd.c' where the 'SIGPIPE' signal is not correctly ignored. This can be exploited to crash a vulnerable service via a malicious peer terminating a TCP connection prematurely. Upgrade to 1.0.7-pre1: http://sourceforge.net/project/showfiles.php?group_id=14&package_id=174 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:146 Debian: http://www.debian.org/security/2004/dsa-606 Red Hat: http://rhn.redhat.com/errata/RHSA-2004-583.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors nfs-utils 'SIGPIPE' TCP Connection Termination Denial of Service CAN-2004-0946 CAN-2004-1014	Low	Secunia Advisory ID, SA13384, December 7, 2004 Debian Security Advisory DSA-606-1 nfs-utils, December 8, 2004 Red Hat Security Advisory, RHSA-2004:583-09, December 20, 2004 Mandrakelinux Security Update Advisory, MDKSA-2005:005, January 12, 2005 US-CERT VU#698302 **Turbolinux Security Advisory, TLSA-2005-33, March 17, 2005**
Multiple Vendors Daniel Stenberg curl 6.0-6.4, 6.5-6.5.2, 7.1, 7.1.1, 7.2, 7.2.1, 7.3, 7.4, 7.4.1, 7.10.1, 7.10.3-7.10.7, 7.12.1	A buffer overflow vulnerability exists in the Kerberos authentication code in the 'Curl_krb_kauth()' and 'krb4_auth()' functions and in the NT Lan Manager (NTLM) authentication in the 'Curl_input_ntlm()' function, which could let a remote malicious user execute arbitrary code. SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/curl/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Updates available at: http://curl.haxx.se/download/curl-7.13.1.tar.gz **Gentoo: http://security.gentoo.org/glsa/glsa-200503-20.xml** **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors cURL / libcURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows CAN-2005-0490	High	iDEFENSE Security Advisory , February 21, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:048, March 4, 2005 **Gentoo Linux Security Advisory, GLSA 200503-20, March 16, 2005** **Conectiva Linux Security Announcement, CLA-2005:940, March 21, 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	Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows CAN-2004-0888 CAN-2004-0889	High	Security Tracker 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

	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 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-132.html FedoraLegacy: http://download.fedoralegacy.org/redhat/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-213.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.			Fedora Update Notifications, FEDORA-2005-122, 123, 133-136, February 8 & 9, 2005 Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005 Mandrakelinux Security Update Advisories, MDKSA-2005:041-044, February 18, 2005 RedHat Security Advisory, RHSA-2005:132-09, February, 18. 2005 Fedora Legacy Update Advisory, FLSA:2127, March 2, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4, 2005 RedHat Security Advisory, RHSA-2005:213-04, March 4, 2005 SGI Security Advisory, 20050204-01-U, March 7, 2005 **SUSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005**
Multiple Vendors Gentoo Linux; GNU Mailman 2.1-2.1.5; RedHat Fedora Core3 & Core2; Ubuntu Linux 4.1 ppc, ia64, ia32	A Directory Traversal vulnerability exists in 'private.py' due to an input validation error, which could let a remote malicious user obtain sensitive information. Debian: http://security.debian.org/pool/updates/main/m/mailman/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-11.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-136.html SUSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/	GNU Mailman Remote Directory Traversal CAN-2005-0202	Medium	Debian Security Advisory, DSA 674-1, February 10, 2005 Ubuntu Security Notice USN-78-1, February 10, 2005 Fedora Update Notifications FEDORA-2005-131 & 132, February 10, 2005 Gentoo Linux Security Advisory, GLSA 200502-11, February 10, 2005 RedHat Security Advisory, RHSA-2005:136-08, February 10, 2005 Fedora Update Notifications, FEDORA-2005-131 & 132, February 10, 2005 Gentoo Linux Security Advisory, GLSA 200502-11, February 10, 2005 Debian Security Advisories, DSA 674-1 & 674-2, February 10 & 11, 2005 SUSE Security Announcement,

	pool/main/m/mailman/ **Apple:** **http://www.apple.com/support/downloads/securityupdate2005003client.html** There is no exploit code required.			SUSE-SA:2005:007, February 14, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:037, February 14, 2005 Ubuntu Security Notice, USN-78-2 , February 17, 2005 Debian Security Advisory, DSA 674-3, February 21, 2005 **Apple Security Update, APPLE-SA-2005-03-21, March 21, 2005**
Multiple Vendors Gentoo Linux; Lgames LTris 1.0.1	A buffer overflow vulnerability has been in reported in 'chart.c' due to a boundary error when handling the highscore lists, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://lgames.sourceforge.net/download.php?project=LTris&url=SOURCEFORGE/lgames/ltris-1.0.10.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200503-24.xml Currently we are not aware of any exploits for this vulnerability.	Lgames LTris Local Global High Score File Buffer Overflow CAN-2005-0825	High	Secunia Advisory, SA14635, March 21, 2005 Gentoo Linux Security Advisory, GLSA 200503-24, March 20, 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; Avaya S8710/S8700/ S8500/S8300, Converged Communication Server, Intuity LX, MN100, Modular Messaging, Network Routing	A vulnerability exists in the 'load_elf_library()' function in 'binfmt_elf.c' because memory segments are not 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 Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-034_RHSA-2005-016RHSA-2006-017RHSA-2005-043.pdf Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html FedoraLegacy: http://download.fedoralegacy.org/redhat/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Another exploit script has been published.**	Linux Kernel uselib() Root Privileges 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 Avaya Security Advisory, ASA-2005-034, February 8, 2005 Ubuntu Security Notice, USN-57-1, February 9, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005 SUSE Security Announcement, SUSE-SA:2005:010, February 25, 2005 Turbolinux Security Announcement , February 28, 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 2005**

Multiple Vendors Linux kernel 2.6 .10, Linux kernel 2.6 -test1-test11, 2.6-2.6.8	A Denial of Service vulnerability has been reported in the Netfilter code due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Netfilter Memory Leak Denial of Service CAN-2005-0210	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6 -test1-test11, 2.6, 2.6.1 rc1&rc2, 2.6.1-2.6.8	A remote Denial of Service vulnerability has been reported in the Point-to-Point Protocol (PPP) Driver. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ **Trustix: http://http.trustix.org/pub/trustix/updates** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PPP Driver Remote Denial of Service CAN-2005-0384	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 **Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005**
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in 'SYS_EPoll_Wait' due to a failure to properly handle user-supplied size values, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1 **An exploit script has been published.**	Linux Kernel SYS_EPoll_Wait Elevated Privileges CAN-2005-0736	Medium	Security Focus, 12763, March 8, 2005 Ubuntu Security Notice, USN-95-1 March 15, 2005 **Security Focus, 12763, March 22, 2005**
Multiple Vendors SuSE Linux 8.0, i386, 8.1, 8.2, 9.0 x86_64, 9.0-9.2; Wietse Venema Postfix 2.1.3	A vulnerability exists because arbitrary mail with an IPv6 address can be sent to any MX host, which could let a remote malicious user bypass security. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/postfix/ SuSE: ftp://ftp.suse.com/pub/suse/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-152.html** There is no exploit code required.	Postfix IPv6 Security Bypass **CAN-2005-0337**	Medium	SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Ubuntu Security Notice, USN-74-2, February 4, 2005 **RedHat Security Advisory, RHSA-2005:152-04, March 16, 2005**
Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-15.xml **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005 **Ubuntu Security Notice, USN-97-1 March 16, 2005**
Multiple Vendors xli 1.14-1.17	A vulnerability exists due to a failure to manage internal buffers securely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/	XLI Internal Buffer Management CAN-2005-0639	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 **Debian Security Advisory, DSA 695-1, March 21, 2005**

	glsa/glsa-200503-05.xml **Debian:** **http://security.debian.org/pool/updates/main/x/xli/** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors xli 1.14-1.17; xloadimage 3.0, 4.0, 4.1	A vulnerability exists due to a failure to parse compressed images safely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml **Debian:** **http://security.debian.org/pool/updates/main/x/xli/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	XLoadImage Compressed Image Remote Command Execution CAN-2005-0638	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 **Fedora Update Notifications, FEDORA-2005-236 & 237, March 18, 2005** **Debian Security Advisory, DSA 695-1, March 21, 2005**
Novell Evolution 2.0.2, 2.0.3	A remote Denial of Service vulnerability has been reported due to the way messages are processed that contained malformed unicode specifications. Mandrake: http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.	Novell Evolution Remote Denial of Service CAN-2005-0806	Low	Mandrakelinux Security Update Advisory, MDKSA-2005:059, March 17, 2005
OpenSLP OpenSLP 1.0.0-1.0.11, 1.1.5, 1.2.0	Multiple buffer overflow vulnerabilities have been reported when processing malformed SLP (Service Location Protocol) packets, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=1730 SuSE: ftp://ftp.suse.com/pub/suse/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/o/openslp/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-25.xml** Currently we are not aware of any exploits for these vulnerabilities.	OpenSLP Multiple Buffer Overflows CAN-2005-0769	High	SuSE Security Announcement, SUSE-SA:2005:015, March 14, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:055, March 16, 2005** **Ubuntu Security Notice, USN-98-1 March 17, 2005** **Gentoo Linux Security Advisory, GLSA 200503-25, March 20, 2005**
Opera Software Opera 7.54 on Linux with KDE 3.2.3; Gentoo Linux	A vulnerability exists that could permit a remote user to cause the target user to execute arbitrary commands. KDE uses 'kfmclient exec' as the default application for processing saved files. A remote user can cause arbitrary shell commands to be executed on the target system. Opera: http://www.opera.com/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-17.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** A Proof of Concept exploit has been published.	Opera Default 'kfmclient exec' Configuration CAN-2004-1491	High	Zone-H Advisory, ZH2004-19SA, December 12, 2004 Gentoo Linux Security Advisory, GLSA 200502-17, February 14, 2005 **SUSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005**

phpMyAdmin phpMyAdmin 1.x, 2.x	A vulnerability has been reported in the privileges management module due to the way "_" characters are handled, which could let a remote malicious user bypass security restrictions. Updates available at: http://sourceforge.net/project/showfiles.php?group_id=23067 Currently we are not aware of any exploits for this vulnerability.	phpMyAdmin "_" Security Restrictions Bypass CAN-2005-0653	Medium	Secunia Advisory, SA14599, March 16, 2005
SquirrelMail S/MIME Plugin 0.4, 0.5	A vulnerability exists in the S/MIME plug-in due to insufficient sanitization of the 'exec()' function, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.squirrelmail.org/plugin_view.php?id=54 **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	SquirrelMail S/MIME Plug-in Remote Command Execution CAN-2005-0239	High	iDEFENSE Security Advisory, February 7, 2005 US-CERT VU#502328 SUSE Security Announcement, SUSE-SA:2005:015, March 14, 2005 **SUSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005**
Sun Microsystems, Inc. Solaris 7.0 _x86, 7.0, 8.0 _x86, 8.0, 9.0 _x86, 9.0	A buffer overflow vulnerability has been reported in the 'newgrp(1)' command due to insecure copying of user-supplied data, which could let a malicious user execute arbitrary code with ROOT privileges. Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57710-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris NewGRP Buffer Overflow CAN-2005-0816	High	Sun(sm) Alert Notification, 57710, March 16, 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 Gentoo: http://security.gentoo.org/glsa/glsa-200502-02.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-128.html SUSE: ftp://ftp.SUSE.com/pub/SUSE SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Currently we are not aware of any exploits for this vulnerability.	University Of Washington IMAP Server CRAM-MD5 Remote Authentication Bypass CAN-2005-0198	Medium	Gentoo Linux Security Advisory, GLSA 200502-02, February 2, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:026, February 2, 2005 RedHat Security Advisory, RHSA-2005:128-06, February 23, 2005 SUSE Security Announcements, SUSE-SR:2005:006 & SUSE-SA:2005:012, February 25 & March 1, 2005 SGI Security Advisory, 20050301-01-U, March 7, 2005 **US-CERT VU#702777**
Xzabite dyndnsupdate	Multiple buffer overflow vulnerabilities have been reported due to insufficient validation of user-supplied string length, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-27.xml Currently we are not aware of any exploits for this vulnerability.	Xzabite DYNDNSUpdate Multiple Remote Buffer Overflows CAN-2005-0830	High	Gentoo Linux Security Advisory, GLSA 200503-27, March 21, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Belkin Belkin 54G (F5D7130)	Multiple vulnerabilities have been reported: a vulnerability has been reported because UPNP datagrams that contain a URI are transmitted at regular intervals, which could let a remote malicious user obtain access to the URL without authentication; a vulnerability has been reported because SNMP support is enabled under the default configuration, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability has been reported in the SNMP service. No workaround or patch available at time of publishing. There is no exploit code required.	Belkin 54G Wireless Router Multiple Vulnerabilities CAN-2005-0833 CAN-2005-0834 CAN-2005-0835	Low/ Medium (Medium if sensitive information can be obtained)	Security Focus, 12846, March 18, 2005
betaparticle betaparticle blog 2.0, 3.0	Multiple vulnerabilities have been reported: a vulnerability has been reported because the database file is located inside the web root, which could let a remote malicious user obtain sensitive information; and a vulnerability has been reported in the 'upload.asp' and 'myFiles.asp' scripts because a remote malicious user can upload and delete files/images without authentication. For the database file vulnerability: Deny direct access to the database file or move it outside the web root. Update available at: http://www.betaparticle.com/blog/about.html Proofs of Concept exploits have been published.	Betaparticle Blog Multiple Remote Vulnerabilities	Medium	Secunia Advisory, SA14668, March 22, 2005
Ciamos Ciamos RC1, Beta 0.9, 0.9.2 RC1	A vulnerability has been reported in 'highlight.php' due to insufficient sanitization of the 'file' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Ciamos 'Highlight.PHP' Information Disclosure CAN-2005-0828	Medium	IHS Advisory, March 19, 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 Rev. 1.4: Modifications and additions to the Details section. **Revision 1.5:Updated the IOS Software 12.2T available repaired release information in the IOS release table in the Software Versions and Fixes section.** 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 VU#689326 Cisco Security Advisory 63845, Revision 1.4, February 9, 2005 **Cisco Security Advisory 63845, Revision 1.5, March 21, 2005**
CoolForum CoolForum 0.5-0.5.2 beta, 0.7.2, 0.7.3, 0.8	Multiple input validation vulnerabilities have been reported; a vulnerability has been reported in the 'avatar.php' script due to insufficient validation of the 'img' parameter, which could let a remote malicious user execute arbitrary code; a vulnerability has been reported in the 'admin/entete.php' script due to insufficient validation of the 'pseudo' parameter, which could let a remote malicious user inject arbitrary SQL commands; and a vulnerability has been reported in the 'register.php' page due to insufficient validation of the 'login' parameter, which could let a remote malicious user execute arbitrary SQL commands. Updates available at: http://www.coolforum.net/index.php?p=dlcoolforum Proofs of Concept exploits have been published.	CoolForum Multiple Input Validation	High	Security Tracker Alert, 1013474, March 18, 2005
Czaries Network CzarNews 1.13 b	A vulnerability has been reported due to insufficient validation of several scripts which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of	CzarNews Arbitrary Code Execution	High	[In]Security Research Advisory, March 20, 2005

	Concept exploit has been published.			
DataRescue IDA Pro 4.7.0.830	A format string vulnerability has been reported in the debugging functionality when handling loaded dynamic link libraries, 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.	DataRescue IDA Pro Remote Format String CAN-2005-0770	High	Securiteam, March 17, 2005
DeleGate DeleGate 7.7 .0, 7.7.1, 7.8 .0-7.8.2, 7.9.11, 8.3.3, 8.3.4, 8.4.0, 8.5 .0, 8.9-8.9.6, 8.10-8.10.2	Multiple buffer overflow vulnerabilities have been reported due to unspecified errors which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Updates available at: http://www.delegate.org/delegate/download/ Currently we are not aware of any exploits for these vulnerabilities.	DeleGate Multiple Unspecified Buffer Overflows	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14649, March 22, 2005
Ethereal Group Ethereal 0.10-0.10.8	A buffer overflow vulnerability exists due to a failure to copy network derived data securely into sensitive process buffers, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-16.xml **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **RedHat: http://rhn.redhat.com/errata/RHSA-2005-306.html** Exploit scripts have been published.	Ethereal Buffer Overflow CAN-2005-0699	High	Security Focus, 12759, March 8, 2005 Security Focus, 12759, March 14, 2005 Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005 **Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005** **RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005**
Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported in the Etheric dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability has been reported in the GPRS-LLC dissector if the 'ignore cipher bit' option is enabled; a buffer overflow vulnerability has been reported in the 3GPP2 A11 dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and remote Denial of Service vulnerabilities have been reported in the JXTA and sFLow dissectors. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-16.xml **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **RedHat: http://rhn.redhat.com/errata/RHSA-2005-306.html** **A Denial of Service Proof of Concept exploit script has been published.**	Ethereal Etheric/GPRS-LLC/IAPP/JXTA/sFlow Dissector Vulnerabilities CAN-2005-0704 CAN-2005-0705 CAN-2005-0739	Low/ HIgh (High if arbitrary code can be executed)	Ethereal Advisory, enpa-sa-00018, March 12, 2005 Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005 **Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005** **RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005**

Icecast Icecast 2.0-2.0.2, 2.1 .0, 2.2	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported in the XSL parser due to insufficient bounds checks on XSL tags, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code; and a vulnerability has been reported due to a failure to parse XSL files when a request for such a file is appended with a dot '.' character, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Icecast XSL Parser Multiple Vulnerabilities CAN-2005-0837 CAN-2005-0838	Low/ Medium/ High (Low of a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	Security Tracker Alert, 1013475, March 19, 2005
Kayako Web Solutions eSupport 2.3	A Cross-Site Scripting vulnerability has been reported in the 'index.php' script due to insufficient sanitization of multiple parameters, 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.	Kayako ESupport 'Index.PHP' Cross-Site Scripting	High	GulfTech Security Research Advisory, March 22, 2005
Marc Cagninacci McNews 1.0, 1.1 a, 1.1-1.3	A vulnerability has been reported in the 'install.php' script due to insufficient sanitization, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	McNews 'Install.PHP' Arbitrary Code Execution CAN-2005-0800	High	Security Focus, 12835, March 17, 2005
McAfee Active Mail Protection, Active Threat Protection, Active Virus Defense, Active Virus Defense SMB Edition, Active VirusScan, Active VirusScan SMB Edition, GroupShield for Exchange 5.5, 6.0, GroupShield for Lotus Domino, GroupShield for Mail Servers with ePO, InternetSecurity Suite, LinuxShield, Managed VirusScan, NetShield for Netware, PortalShield for Microsoft SharePoint, SecurityShield for Microsoft ISA Server, Virex, VirusScan 1.0, 2.0, 3.0	A buffer overflow vulnerability has been reported in the LHA parser, due to insufficient bounds checking of LHA type two header file name fields, which could let a remote malicious user execute arbitrary code with SYSTEM privileges. The vendor recommends applying the latest .DAT files and updating to AV scanning engine version 4400. Currently we are not aware of any exploits for this vulnerability.	McAfee Antivirus Library LHA Remote Buffer Overflow CAN-2005-0643 CAN-2005-0644	High	Internet Security Systems Protection Advisory March 17, 2005 US-CERT VU#361180

Mozilla Mozilla 1.7.x and prior Mozilla Firefox 1.x and prior Mozilla Thunderbird 1.x and prior	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird. These can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious people to conduct spoofing attacks, disclose and manipulate sensitive information, and potentially compromise a user's system. Firefox: Update to version 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.6 version. Thunderbird: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.0.1 version. Fedora update for Firefox: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml **SUSE: ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	Mozilla / Firefox / Thunderbird Multiple Vulnerabilities CAN-2005-0255 CAN-2005-0584 CAN-2005-0585 CAN-2005-0587 CAN-2005-0588 CAN-2005-0589 CAN-2005-0590 CAN-2005-0592 CAN-2005-0593	High	Mozilla Foundation Security Advisories 2005-14, 15, 17, 18, 19, 20, 21, 24, 28 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 **SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005**
Multiple Vendors Mozilla Firefox 1.0; Gentoo Linux; **Thunderbird 0.6, 0.7- 0.7.3, 0.8, 0.9, 1.0, 1.0.1; Netscape Netscape 7.2**	There are multiple vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. A fix is available via the CVS repository Fedora: ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml **Thunderbird: http://download.mozilla.org/?product=thunderbird-1.0.2&os=win<=en-US** A Proof of Concept exploit has been published.	Mozilla Firefox Multiple Vulnerabilities CAN-2005-0230 CAN-2005-0231 CAN-2005-0232	High	Security Tracker Alert ID: 1013108, February 8, 2005 Fedora Update Notification, FEDORA-2005-182, February 26, 2005 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 **Security Focus, 12468, March 22, 2005**
Mozilla Mozilla 1.7.3 Mozilla Firefox 1.0 for Windows	A vulnerability exists that could let remote malicious users trick users into downloading malicious files. This is because the the browser uses the different criteria to determine the the file type when saving the downloaded file. Updated versions are available. Mozilla Firefox 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla 1.7.5: http://www.mozilla.org/products/mozilla1.x/ Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo:	Mozilla / Firefox Download Spoofing Vulnerability CAN-2005-0586	Medium	Secunia SA13258, March 1, 2005 Mozilla Foundation Security Advisory 2005-22 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 **SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005**

	http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Mozilla Firefox 1.0; **Gentoo Linux; Thunderbird 0.6, 0.7-0.7.3, 0.8, 0.9, 1.0, 1.0.1, Netscape 7.2**	There are multiple vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. A fix is available via the CVS repository Fedora: ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Thunderbird:** **http://download.mozilla.org/?product=thunderbird-1.0.2&os=win&lang=en-US** A Proof of Concept exploit has been published.	Multiple Vendors Mozilla Firefox Multiple Vulnerabilities CAN-2005-0230 CAN-2005-0231 CAN-2005-0232	High	Security Tracker Alert ID: 1013108, February 8, 2005 Fedora Update Notification, FEDORA-2005-182, February 26, 2005 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 **SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005** **Security Focus, 12468, March 22, 2005**
Multiple Vendors OpenPGP	A vulnerability exists that could permit a remote malicious user to conduct an adaptive-chosen-ciphertext attack against OpenPGP's cipher feedback mode. The flaw is due to an ad-hoc integrity check feature in OpenPGP. A solution will be available in the next release of the product. SUSE: ftp://ftp.SUSE.com/pub/SUSE **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** A Proof of Concept exploit has been published.	Multiple Vendors OpenPGP CFB Mode Vulnerable to Cipher-Text Attack CAN-2005-0366	Medium	US-CERT VU#303094 SUSE Security Summary Report, SUSE-SR:2005:007, March 4, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:057, March 16, 2005**
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability was reported in the CREATE FUNCTION command that could let an authenticated user gain mysql user privileges on the target system and permit the user to execute arbitrary code. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/downloads/index.html **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-19.xml** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Trustix:** **http://http.trustix.org/pub/trustix/updates/**	MySQL CREATE FUNCTION Remote Code Execution Vulnerability CAN-2005-0709	High	Security Tracker Alert ID: 1013415, March 11, 2005 **Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005** **Ubuntu Security Notice, USN-96-1 March 16, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005** **Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005**

	A Proof of Concept exploit has been published.			
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability has been reported that could let local malicious users gain escalated privileges. This is because the "CREATE TEMPORARY TABLE" command can create insecure temporary files. The vulnerabilities have been fixed in version 4.0.24 (when available): http://dev.mysql.com/downloads/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-19.xml** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** A Proof of Concept exploit has been published.	MySQL Escalated Privilege Vulnerabilities CAN-2005-0711	Medium	Secunia SA14547, March 11, 2005 **Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005** **Ubuntu Security Notice, USN-96-1 March 16, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005** **Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005**
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	An input validation vulnerability was reported in udf_init() that could let an authenticated user with certain privileges execute arbitrary library functions on the target system. The udf_init() function in 'sql_udf.cc' does not properly validate directory names. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/downloads/index.html **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-19.xml** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** A Proof of Concept exploit has been published.	MySQL udf_init() Path Validation Vulnerability CAN-2005-0710	High	Security Tracker Alert ID: 1013414, March 11, 2005 **Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005** **Ubuntu Security Notice, USN-96-1 March 16, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005** **Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005**
NetWin SurgeMail 1.8 g3, 1.8 e, 1.8 d, 1.8 b3, 1.8 a, 1.9 b2, 1.9, 2.0 g2, 2.0 e, 2.0 c, 2.0 a2, 2.1 c7, 2.1 a, 2.2 g3, 2.2 g2, 2.2 c9, 2.2 c10, 2.2 a6, 3.0 a	Two vulnerabilities have been reported in the webmail functionality and 'user.cgi' due to unspecified errors. The impact was not specified. Updates available at: http://www.netwinsite.com/download.htm Currently we are not aware of any exploits for these vulnerabilities.	NetWin SurgeMail Multiple Remote Unspecified Vulnerabilities	Not Specified	Secunia Advisory, SA14658, March 22, 2005
Novell Netware 6.5 SP2 & SP3	A vulnerability has been reported in the 'xvesa' code due to insufficient authentication routines, which could let a remote malicious user bypass certain security restrictions and obtain gain access to the server Console. Patches available at: http://support.novell.com/servlet/filedownload/sec/ftf/xvsft1.exe There is no exploit code required.	Novell Netware Xsession Security Bypass CAN-2005-0819	Medium	Technical Information Document, TID2971038, March 16, 2005
Phorum Phorum 5.0.14, 3.1-3.1.2, 3.2-3.2.8, 3.3.1 - 3.3.2, 3.4-3.4.8, 5.0.3 BETA, 5.0.7 BETA,	A response splitting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user mount various kinds of attacks including Cross-Site Scripting, Web Cache Poisoning, Browser cache poisoning, Hijack pages, etc. Upgrades available at: http://phorum.org/downloads/	Phorum HTTP Response Splitting	Medium	Positive Technologies Advisory, SA-20050322, March 22, 2005

5.0.9-5.0.13	phorum-5.0.15a.tar.gz A Proof of Concept exploit has been published.			
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/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/** There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHP Multiple Remote Vulnerabilities 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 Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005 **Ubuntu Security Notice, USN-99-1 March 18, 2005**
phpAdsNew phpAdsNew 2.0.4 -pr1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. **Upgrade available at: http://prdownloads.sourceforge.net/phpadsnew/phpAdsNew-2.0.4-pr2.tar.gz?download** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPAdsNew AdFrame.PHP Cross-Site Scripting CAN-2005-0791	High	Security Focus, 12803, March 14, 2005 **Security Focus, 12803, March 16, 2005**
PHP-Fusion PHP-Fusion 4.00, 4.0 1, 5.0 1 Service Pack, 5.0	A vulnerability has been reported in the 'setuser.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. Patch available at: http://www.php-fusion.co.uk/news.php?readmore=190 An exploit script has been published.	PHP-Fusion Setuser.PHP HTML Injection CAN-2005-0829	High	Security Focus, 12853, March 18, 2005

phpmyfamily phpmyfamily 1.4	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPMyFamily Multiple SQL Injection	High	ADZ Security Team Advisory, March 20, 2005
phpopenchat.org PHPOpenChat 2.3.4, 3.0.1	Multiple vulnerabilities have been reported: a vulnerability has been reported in 'contrib/yabbse/poc.php' due to insufficient verification of the 'sourcedir' parameter, which could let a remote malicious user execute arbitrary code; a vulnerability has been reported in '/phpopenchat/contrib/phpbb/alternative2/phpBB2_root/poc_loginform.php', because the 'extension.inc' file is included relative to the 'phpbb_root_path' parameter value, which could let a remote malicious user execute arbitrary PHP code; and vulnerabilities have been reported in '/phpopenchat/contrib/phpbb/poc.php,' '/phpopenchat/contrib/phpnuke/ENGLISH_poc.php,' '/phpopenchat/contrib/phpnuke/poc.php,' and '/phpopenchat/contrib/yabbse/poc.php,' which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	PHPOpenChat Multiple Remote Code Execution	High	Albania Security Clan Advisory, March 15, 2005
PHP-post Web Forum 0.1-0.3, 0.21, 0.22, 0.32	Multiple remote input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code and a vulnerability has been reported which could let a remote malicious user spoof usernames. Upgrades available at: http://www.php-post.co.uk/files/phpp.zip There is no exploit code required.	PHP-Post Multiple Remote Input Validation CAN-2005-0831 CAN-2005-0832	High	Security Focus, 12845, March 18, 2005
PunBB PunBB 1.2.3	A vulnerability has been reported due to insufficient validation of the 'email' and 'Jabber' fields, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PunBB Input Validation CAN-2005-0818	High	Security Tracker Alert, 1013446, March 16, 2005
RealNetworks RealPlayer prior to 6.0.12.1059	A vulnerability in the processing of WAV files could let a remote malicious user execute arbitrary code. A special WAV file could trigger a buffer overflow and execute arbitrary code. Updates available at: http://service.real.com/help/faq/security/050224_player/EN/ SUSE: ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/RealPlayer-10.0.3-0.1.i586.rpmcf95cd77f9abda58abff3 b488c55a515 **RedHat: http://rhn.redhat.com/errata/RHSA-2005-299.html** Currently we are not aware of any exploits for this vulnerability.	RealNetworks RealPlayer WAV File Error Permits Remote Code Execution CAN-2005-0611	High	RealPlayer Release Notes March 1, 2005 SUSE-SA:2005:014, March 9, 2005 **RedHat Security Advisory, RHSA-2005: 299-06, March 21, 2005**
RunCMS RunCMS 1.1 (formerly E-Xoops E-Xoops 1.0 5r3)	Several vulnerabilities have been reported: a vulnerability has been reported in 'highlight.php' due to insecure storage of sensitive information, which could let a malicious user obtain sensitive information; and a vulnerability has been reported in the 'convertorderbytrans()' function in 'viewcat.php', which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	RunCMS Information Disclosures CAN-2005-0827 CAN-2005-0828	Medium	IHS Iran Hackers Sabotage Public advisory, March 18, 2005

Samsung DSL Modem SMDK8947v1.2	Multiple vulnerabilities have been reported: a vulnerability has been reported due to a failure to block access to sensitive files, which could let a remote malicious user obtain sensitive information; and a vulnerability has been reported due to a default backdoor account, which could let a remote malicious user obtain administrative privileges. No workaround or patch available at time of publishing. There is no exploit code required.	Samsung DSL Modem Multiple Remote Vulnerabilities	Medium/ High (High if administrative access can be obtained)	Security Focus, 12864, March 21, 2005
Subdreamer Subdreamer Light 1.0.1-1.0.3, 1.1.3-1.1.5	A vulnerability has been reported vulnerability in 'index.php' when 'magic_quotes_gpc' is enabled due to insufficient sanitization of various global variables, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Subdreamer SQL Injection CAN-2005-0805	High	GHC Advisory, March 18, 2005
Sun Microsystems, Inc. Sun Java 2 Runtime Environment 1.3 0_01-1.3 0_05, 1.3 .0, 1.3.1 _08, 1.3.1 _04, 1.3.1 _01a, 1.3.1 _01, 1.3.1, 1.4.1, 1.4.2 _01-1.4.2 _06, 1.4.2, Java Web Start 1.2	A vulnerability has been reported due to insufficient validation of user-supplied input before considered as trusted, which could let a remote malicious user obtain obtain elevated privileges. Upgrades available at: http://java.sun.com/j2se/ Currently we are not aware of any exploits for this vulnerability.	Sun Java Web Start System Remote Unauthorized Access CAN-2005-0836	Medium	Sun(sm) Alert Notification, 57740, March 16, 2005
Symantec Symantec Enterprise Firewall 7.0 Solaris, 7.0 NT/2000, 8.0 Solaris. 8.0 NT/2000, Gateway Security 5300, 5300 1.0, 5400 2.0, 2.0.1, VelociRaptor 1100, 1100 1.5, 1200, r 1200 1.5, 1300, 1300 1.5	A vulnerability has been reported in the DNS proxy (DNSd) due to an unspecified error. which could let a remote malicious user poison the DNS cache. Hotfixes available at: http://www.symantec.com/techsupp Currently we are not aware of any exploits for this vulnerability.	Symantec Gateway Security Remote DNS Cache Poisoning CAN-2005-0817	Medium	Symantec Security Advisory, SYM05-005 March 15, 2005
The Rusted Gate TRG News 3.0	A vulnerability has been reported due to insufficient validation of several scripts which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	TRG News Script Arbitrary Code Execution	High	[In]Security Research Advisory, March 20, 2005
ZPanel ZPanel 2.0, 2.5 beta9 & beta 10, 2.5 beta	Multiple vulnerabilities have been reported: a vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'uname' parameter, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability has been reported because installation scripts are not properly removed after installation, which could let a remote malicious user reinstall an affected installation. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	ZPanel Multiple SQL Injection and File Include CAN-2005-0792 CAN-2005-0793 CAN-2005-0794	High	Secunia Advisory, SA14602, March 16, 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
March 22, 2005	dbmac-0.2.tar.gz	N/A	A database of MAC prefixes for spoofing your MAC address in Linux. Ideal for in war driving situations.
March 22, 2005	goodtech.c gtscrash.c.txt	No	Proof of Concept exploit for the GoodTech Systems Telnet Server for Windows NT/2000/XP/2003 Remote Buffer Overflow vulnerability.
March 22, 2005	krad.c	Yes	Script that exploits the Linux Kernel SYS_EPoll_Wait Elevated Privileges vulnerability.
March 22, 2005	mailenable.tar.gz	No	Denial of service exploit for the MailEnable Standard SMTP Format String Vulnerability.
March 22, 2005	phpMyFamily140.txt	No	Proof of Concept exploit for the PHPMyFamily Multiple SQL Injection vulnerability.
March 22, 2005	psnup.pl.txt	No	Proof of Concept exploit for PostScript utility vulnerability.
March 22, 2005	pwned.c	Yes	Script that exploits the Linux Kernel uselib() Root Privileges vulnerability.
March 22, 2005	rkhunter-1.2.3.tar.gz	N/A	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
March 22, 2005	szapper.c	N/A	StealthZapper is a less-detectable log wiper that attempts to leave wtmp and utmp "cleaner" looking by not simply leaving a blank hole where the offending data was deleted from.
March 21, 2005	funlabsboom.zip	No	Proof of Concept exploit for the FUN labs Games Denial of Service Vulnerability.
March 21, 2005	ocean_poc.pl	Yes	Perl script that exploits the Code Ocean Ocean FTP Server Remote Denial of Service vulnerability.
March 21, 2005	xosx-cf.c	Yes	Script that exploits the Apple Mac OS X Multiple Vulnerabilities.
March 19, 2005	phpbbexp.cpp phpBBsession.txt	No	Exploit for the phpbb vulnerability.
March 19, 2005	PHP-Fusion_Exploit.txt	Yes	Exploit for the PHP-Fusion 'Setuser.PHP' HTML Injection vulnerability.
March 18, 2005	PHPOC_XSS.txt	No	Proof of Concept exploit for the PHPOpenChat Multiple HTML Injection vulnerabilities.
March 17, 2005	activeCam.txt	No	Exploit for the PY Software Active Webcam Webserver Remote Denials of Service & Information Disclosure vulnerability.
March 17, 2005	eth2.c	Yes	Exploit for the Ethereal IAPP dissector remote buffer overflow vulnerability.
March 17, 2005	ethereal-3g-a11.c	Yes	Proof of Concept remote root exploit for the Ethereal CDMA2000 A11 protocol dissector stack overflow vulnerability.
March 17, 2005	IdaPOC.zip	No	Proof of Concept exploit for the IDA Pro Format String Vulnerability.
March 17, 2005	iPool.c	No	Script that exploits the ThePoolClub IPool Insecure Local Credential Storage vulnerability.
March 17, 2005	iSnooker.c	No	Script that exploits the ThePoolClub ISnooker Insecure Local Credential Storage vulnerability.
March 17, 2005	luxman_ex2.pl	Yes	Exploit for the Frank McIngvale LuxMan Buffer Overflow vulnerability.
March 17, 2005	platinumDoS.c	No	Perl script that exploits the PlatinumFTPServer Malformed User Name Connection Remote Denial of Service vulnerability.
March 17, 2005	silentdoor.tar.gz	N/A	A connectionless, PCAP-based backdoor for linux that uses packet sniffing to bypass netfilter.

[back to top]

Trends

- A hack was revealed by Netcraft, a UK security company, that attempts to hijack a website frame on a legitimate banking site. The new 'cross-frame' scripting approach injects content onto a real web page which makes it difficult to detect. For more information, see "New style of phishing attack discovered" located at: http://www.techworld.com/security/news/index.cfm?NewsID=3348
- According to latest Symantec Internet Security Threat Report, the UK has more than a quarter (25.2 per cent) of all bots virus-infected, zombie PCs under the control of crackers and used for malicious purposes like identity theft and online fraud with the US (24.6 percent) and China (7.8 percent) in second and third place. For more information, see "Britain tops zombie PC charts" located at: http://www.securityfocus.com/news/10730 and Symantec Report: http://enterprisesecurity.symantec.com/content.cfm?articleid=1539 .
- Symantec's biannual Internet Security Threat Report said one of the fastest-growing threats is from "phishing" attacks, which lure people to Web sites that appear to be owned by banks or other firms and dupe them into giving passwords, credit card numbers or other key information. Viruses, spam and other computer security threats are growing at a rapid rate, much of it aimed at stealing personal or confidential information. For more information, see: " Hacker Threats, Spam Still Growing" located at: http://www.newsfactor.com/story.xhtml?story_title=Hacker_Threats__Spam_Still_Growing&story_id=31581 and Symantec Report: http://enterprisesecurity.symantec.com/content.cfm?articleid=1539 .
- According to summit attendees at the second annual "Wireless On Wall Street" conference, encrypted fully authenticated wireless network remains high on the list. Financial-services companies are under constant pressure from customers and employees to implement wireless technology because of the convenience it offers. For more information, see " Wireless Security Top Concern For Financial Companies" located at:

  http://www.informationweek.com/story/showArticle.jhtml?articleID=159903610&tid=13692
- Worms and viruses are increasingly infecting wireless phones, PDAs and other devices. Even though mobile viruses, to date, haven't caused considerable damage to enterprises, there is reason for concern. A recent survey conducted by security specialist netSurity for RSA Security Inc. found that in the business district of London, the number of wireless LANs increased by 62% in 2004, with access points growing to 1,751 from 1,078. At the same time, security on the wireless networks got worse, leaving 36% of the companies open to potential attack, up from 25% in 2003. For more information see, "IT managers need to prepare for mobile viruses" located at: http://www.computerworld.com/mobiletopics/mobile/story/0,10801,100409,00.html
- Instant messaging (IM) security threats are growing by 50 percent each month and could potentially spread across the globe in seconds.

According to research from anti-virus firm F-Secure, virus writers are targeting instant messaging application due to their ability to spread malicious code faster than email worms. For more information, see "IM viruses increase by 50% a month" located at: http://www.vnunet.com/news/1162017

- Federal and state law enforcement officials say sophisticated criminals have begun to use the unsecured Wi-Fi networks of unsuspecting consumers and businesses to help cover their tracks in cyberspace. Experts say most households with Wi-Fi connections never turn on any of the features, available in almost all Wi-Fi routers, that change the system's default settings, conceal the connection from others and encrypt the data sent over it. For more information, see "Growth of wireless Internet opens new path for thieves" located at: http://www.nytimes.com/2005/03/19/technology/19wifi.html.
- Kaspersky Labs said there is evidence that a battle is shaping up between rival cyber gangs over the newest turf, infectable PCs. A new Trojan -- dubbed Small.bi -- removes a number of .exe files associated with Trojan-like names before it installs itself. For more information, see "Hacker turf war will lead to large e-crime gangs" located at: http://www.techweb.com/wire/security/159902363.

[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	Bagle-BJ	Win32 Worm	Stable	January 2005
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Netsky-Q	Win32 Worm	Stable	March 2004
5	Zafi-B	Win32 Worm	Stable	June 2004
6	Netsky-D	Win32 Worm	Stable	March 2004
7	Netsky-Z	Win32 Worm	Stable	April 2004
8	Netsky-B	Win32 Worm	Stable	February 2004
9	Bagle-AU	Win32 Worm	Stable	October 2004
10	Bagle.BB	Win32 Worm	Stable	September 2004

Table Updated March 22, 2005

Viruses or Trojans Considered to be a High Level of Threat

- Nothing significant to report.

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.Tuimer		Trojan
Crowt.B	W32/Crowt.B.worm	Win32 Worm
Del-470	Del-471 TR/KillFiles.HQ Trj/Delfiles.R Troj/Cyberno-A Trojan.KillFiles.HQ Trojan.Win32.KillFiles.hq TROJ_KILLFILE.HQ W32/Killfiles.H Win32.KillFiles.AF	Trojan
Downloader.Newest		Trojan
Drever.A	SymbOS/Drever SymbOS/Drever.A SYMBOS_DREVER.A	Symbian OS Worm
Drever.B	SymbOS/Drever.B	Symbian OS Worm
Drever.C	SymbOS/Drever.C	Symbian OS Worm
Locknut.B	SymbOS/Locknut.B	Symbian OS Worm

Mydoom.BH	W32/Mydoom.BH.worm	Win32 Worm
Mytob.E	W32/Mytob.E.worm	Win32 Worm
Proxy-Agent.e	Troj/Iyus-H Trojan Trojan-Proxy.Win32.Agent.di TROJ_MSGINA.B Win32.Reign.AO	Trojan
PWSteal.Bancos.R		Trojan
PWSteal.Bancos.S	Trojan-Downloader.Win32.Dadobra.n	Trojan
Skulls.F	SymbOS/Skulls.F	Symbian OS Worm
StartPage-GT		Win32 Worm
Troj/BagDl-Gen		Trojan
Troj/Bancos-BU	TROJ_BANCOS.SE Trojan-Spy.Win32.Banker.lw	Trojan
Troj/Banker-BZ		Trojan
Troj/Banker-HE	Trojan-Spy.Win32.Banker.he	Trojan
Troj/Dloader-JQ		Trojan
Troj/Feutel-B	Backdoor.Win32.Hupigon.j	Trojan
Troj/HideDial-D	Trojan-Downloader.Win32.Tibser.c Trojan.Downloader.Tibser-3	Trojan
TROJ_ASH.A	Ash PWSteal.Bankash.D Troj/BankAsh-C	Trojan
TROJ_ASH.B	PWS-Banker.j.dll PWSteal.Bankash.D Win32.Bankash.D	Trojan
Trojan.Alpiok		Trojan
Trojan.Domcom	Troj/Domcom-C TROJ_DOMCOM.D	Trojan
Trojan.Eaghouse		Trojan
Trojan.Eaghouse.B		Trojan
Trojan.Goldun.D		Trojan
Trojan.Magise		Trojan
Trojan.Mdropper		Trojan
Trojan.Prevert		Trojan
Trojan.Sientok		Trojan
VBS.Scafene@mm		Visual Basic Worm
VBS/LoveLet-AA		Visual Basic Worm
W32.Kelvir.I		Win32 Worm
W32.Mydoom.BG@mm		Win32 Worm
W32.Mytob.H@mm		Win32 Worm
W32.Mytob.I@mm		Win32 Worm
W32.Randex.CZZ		Win32 Worm
W32.Serflog.C	W32/Crog.worm WORM_FATSO.C	Win32 Worm
W32/Demotrayo.worm	Email-Worm.Win32.LovGate.W Trojan.Win32.Dtray.a Win32.HLLW.Demot	Win32 Worm
W32/Domwis-I	Backdoor.Win32.Wisdoor.ao BackDoor-AOZ	Win32 Worm
W32/MyDoom-BH		Win32 Worm
W32/Myfip-K	W32/Myfip.worm.q WORM_MYFIP.I	Win32 Worm
W32/Mytob-B		Win32 Worm
W32/Netsky-AD		Win32 Worm
W32/Poebot-K		Win32 Worm
W32/Rbot-YB	backdoor.win32.rbot.gen w32/sdbot.worm.gen.i worm_rbot.aub worm_rbot.gen trojan.mybot.gen-77	Win32 Worm
W32/Rbot-YN	Backdoor.Win32.Rbot.lp W32/Sdbot.worm.gen.h	Win32 Worm
W32/Rbot-YO		Win32 Worm
W32/Rbot-YV		Win32 Worm
W32/Rbot-YY	Backdoor.Win32.Rbot.lm	Win32 Worm
W32/Sdbot-SB		Win32 Worm
W32/Sdbot-WE	Backdoor.Win32.SdBot.gen	Win32 Worm

W32/Sumom-C	M-Worm.Win32.Sumom.c	Win32 Worm
Win32.Bropia.U		Win32 Worm
Win32.Bropia.V		Win32 Worm
Win32.Elitper.A		Win32 Worm
Win32.Harbag.X		Win32 Worm
Win32.Lioten.KX		Win32 Worm
Win32.Mydoom.BI		Win32 Worm
Win32.SilentCaller.D		Win32 Worm
Win32.Startpage.NS		Win32 Worm
WORM_BUCHON.E	W32/Buchon Win32/NewMalware.gen!	Win32 Worm
WORM_CROWT.B		Win32 Worm
WORM_MYDOOM.AT	W32.Mydoom.BG@mm W32/Mydoom W32/MyDoom-BH Win32.Mydoom.BI Win32/Mydoom.AT@mm	Win32 Worm
WORM_MYTOB.G	W32.Mydoom.gen@mm W32/Mydoom Win32.Mytob.G	Win32 Worm
WORM_MYTOB.H	Exploit-DcomRpc W32.Mydoom.gen@mm Win32.Lioten	Win32 Worm
WORM_TOXBOT.A	MS03-026_Exploit!Trojan W32.Toxbot Win32.Toxbot.W Worm:Win32/Codbot.L	Win32 Worm

[back to top]

Last updated March 23, 2005