US-CERT National Cyber Alert System

SB04-273-Summary of Security Items from September 22 through September 28, 2004

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.

- Symantec Enterprise Firewall/VPN Appliance Multiple Remote Denials of Service & Configuration Modification
- Symantec ON Command Default Usernames & Passwords
- YaBB 1 Gold Multiple Input Validation
- Yahoo! Store Commerce System Price Modification
- YPOPs! Buffer Overflows

Recent Exploit Scripts/Techniques
Trends
Viruses/Trojans

Bugs, Holes, & Patches

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

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

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

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

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
ActivePost Standard 3.0, 3.1	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists due to an error in the integrated file server; a Directory Traversal vulnerability exists due to an input validation error in the file server, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the conference menu, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploit scripts have been published.	ActivePost Messenger Multiple Remote Vulnerabilities	Low/Medium (Medium if sensitive information can be obtained)	Secunia Advisory, SA12642, September 24, 2004
Alt-N Technologies MDaemon 6.5.1	Multiple buffer overflow vulnerabilities exist when a specially crafted SAML, SOML, SEND, or MAIL command is submitted to SMTP port or when a specially crafted LIST command is submitted to the IMAP service due to insufficient validation, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept Denial of Service exploits have been published.	MDaemon IMAP/SMTP Server Multiple Remote Buffer Overflows	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011386, September 22, 2004
BroadBoard.com Broadboard ASP Message Board 1.x	Vulnerabilities exist in the 'keywords' parameter in 'search.asp,' the 'handle' parameter in 'profile.asp,' the 'txtUserHandle' parameter in 'reg2.asp,' and the 'txtUserEmail' parameter in 'forgot.asp' due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Broadboard Input Validation	High	SecurityTracker Alert ID, 1011419, September 27, 2004
Computer Associates Unicenter Management Portal 2.0, 3.1	A vulnerability exists in the 'Forgot your Password?' link on the management portal interface, which could let a remote malicious user obtain sensitive information. The vendor recommends that you disable the 'Forgot Password' feature by adding the following line to the '[PORTAL_INSTALL]\properties\local.properties' file: show.passwords.in.api=false Then, restart the portal after manually editing the file. There is no exploit code required.	Unicenter Management Portal Username Disclosure	Medium	SecurityTracker Alert ID, 1011381, September 22, 2004
Emulive Imaging Corporation EmuLive Server4	Multiple vulnerabilities exist: a vulnerability exists due to an error in the handling of session IDs, which could let a remote malicious user bypass user authentication to obtain access to the administrator section; and a remote Denial of Service vulnerability exists when handling incoming traffic on port 66/tcp if a malicious user submits a sequence of eight or more carriage returns.	EmuLive Server4 Vulnerabilities	Low/High (High if administrative access can be obtained)	GulfTech Security Research Advisory, September 21, 2004

	No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.			
Full Revolution aspWebAlbum 3.2, aspWebCalendar 4.5, aspWebHeadlines 1.1, aspWebMail 1.0	Multiple SQL injection vulnerabilities exist due to insufficient sanitization of user-supplied input prior to including it in an SQL query, 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.	Full Revolution aspWebCalendar & aspWebAlbum Multiple SQL Injection	Medium	Bugtraq, September 23, 2004
Hewlett Packard Company StorageWorks Command View XP 1.7 B, 1.7 A, 1.8 B, 1.8 A, 1.11.02, 1.11, 1.11.1, 1.30 .00, 1.40 .04, 1.40 .01, 1.51 .00, 1.52 .00, 1.53 .05a, 1.53.01a, 1.53 .00, 1.60 .00	A vulnerability exists because a local malicious user user on a management station may be able to bypass access restrictions. Upgrades available at: http://hprc.external.hp.com We are not aware of any exploits for this vulnerability.	HP StorageWorks Command View XP Restriction Bypass	Medium	HP Security Bulletin, HPSBST01071, September 24, 2004
Illustrate dBpowerAMP Audio Player 2.0	Several buffer overflow vulnerabilities exist when a specially crafted '.pls' and '.m3u' playlist and a '.mcc' dBpoweramp Music Collection file is submitted, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	dBpowerAMP Audio Player Buffer Overflows	High	GulfTech Security Research Team Advisory, September 28, 2004
Illustrate dBpowerAMP Music Converter 10.0	Several vulnerabilities exist: buffer overflow vulnerabilities exist when a specially crafted '.pls' and '.m3u' playlist and a '.mcc' dBpoweramp Music Collection file is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists when the Music Converter is integrated into the Windows shell and a specially crafted playlist is submitted, which could let a remote malicious user cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	dBpowerAMP Music Converter Buffer Overflows	Low/High (High if arbitrary code can be executed)	GulfTech Security Research Team Advisory, September 28, 2004
LeadMind Development PopMessenger 1.60	A remote Denial of Service vulnerability exists due to a failure to handle certain characters. Upgrade available at: http://www.leadmind.com/pmesseng.exe Proof of Concept exploit script has been published.	LeadMind Pop Messenger Remote Denial of Service	Low	Bugtraq, September 21, 2004
Microsoft Microsoft .NET Framework 1.x, Digital Image Pro 7.x, 9.x, Digital Image Suite 9.x, Frontpage 2002, Greetings 2002, Internet Explorer 6, Office 2003 Professional Edition, 2003 Small Business Edition, 2003 Standard Edition, 2003 Student and Teacher Edition, Office XP, Outlook 2002, 2003, Picture It! 2002, 7.x, 9.x, PowerPoint 2002, Producer for Microsoft Office PowerPoint 2003, Project 2002, 2003, Publisher 2002, Visio 2002, 2003, Visual Studio .NET 2002, 2003, Word 2002; Avaya DefinityOne Media Servers, IP600 Media Servers, S3400 Modular Messaging, S8100 Media Servers	A buffer overflow vulnerability exists in the processing of JPEG image formats, which could let a remote malicious user execute arbitrary code. Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx **More Proofs of Concept exploit scripts have been published.**	Microsoft JPEG Processing Buffer Overflow CVE Name: CAN-2004-0200	High	Microsoft Security Bulletin, MS04-028, September 14, 2004 US-CERT Vulnerability Note VU#297462, September 14, 2004 Technical Cyber Security Alert TA04-260A, September 16, 2004 SecurityFocus, September 17, 2004 **SecurityFocus, September 28, 2004**
Microsoft SQL Server 7.0 SP3 & prior	A remote Denial of Service vulnerability exists in 'mssqlserver' when a malicious user submits a large buffer with that contains specially crafted data. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft SQL Server Remote Denial of Service	Low	SecurityTracker Alert ID, 1011434, September 28, 2004
Nettica Corporation Intellipeer Email Server 1.x	A vulnerability exists because the POP3 mail server returns different error messages in response to login attempts depending on whether the supplied username is valid or invalid, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Intellipeer Email Server User Account Disclosure	Medium	Secunia Advisory, SA12661, September 27, 2004

PD9 Software MegaBBS 2.x	Multiple vulnerabilities exist: a vulnerability exists in 'thread-post.asp' due to insufficient validation of the 'fid' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in 'ladder-log.asp' due to insufficient validation of the 'sortdir' and 'criteria' parameters, which could let a remote malicious user execute arbitrary code. Update available at: http://www.pd9soft.com/ Proofs of Concept exploits have been published.	MegaBBS Input Validation	High	SecurityTracker Alert ID, 1011420, September 27, 2004
Pinnacle Systems ShowCenter 1.51	A remote Denial of Service vulnerability exists in the 'Skin' parameter due to insufficient sanity checks. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ShowCenter Web Interface Skin Denial Of Service	Low	Bugtraq, September 21, 2004
Sierra Entertainment, Inc. Lords of the Realm III	A remote Denial of Service vulnerability exists when handling nicknames of excessive length and the server is in 'lobby mode.' No workaround or patch available at time of publishing. An exploit script has been published.	Lords of the Realm III Nickname Remote Denial of Service	Low	SecurityFocus, September 20, 2004
Sophos Anti-Virus 3.78 d, 3.78-3.85, Small Business Suite 1.0	A vulnerability exists because malicious code within a filename that uses a reserved MS-DOS device name is not detected by the on-demand scanning feature and the real-time on-access protection feature, which could let a remote malicious user create code that will evade the anti-virus detection capabilities. Update available at: http://www.sophos.com/support/updates.html There is no exploit code required.	Sophos Anti-Virus Reserved MS-DOS Name Scan Evasion CVE Name: CAN-2004-0552	High	iDEFENSE Security Advisory, September 22, 2004
Virtual Projects Chatman 1.5.1 RC1 & prior	A remote Denial of Service vulnerability exists due to an input validation error when a malicious user submits a specially crafted packet that contains an overly large value in the data size field. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ChatMan Input Validation Remote Denial of Service	Low	SecurityTracker Alert ID, 1011431, September 27, 2004
Web Wiz Guide Web Wiz Internet Search Engine	A vulnerability exists in the 'common.inc' file, which could let a remote malicious user obtain sensitive information including the administrative password. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Web Wiz Internet Search Engine Database Disclosure	High	Security .Net Information (snilabs) Advisore, September 26, 2004
Web Wiz Guide Web Wiz Journal	A vulnerability exists because the administrator's unencrypted password is contained in the database, 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.	Web Wiz Journal Database Disclosure	High	Security .Net Information (snilabs) Advisore, September 26, 2004
Zinf Zinf 2.2.1	A buffer overflow vulnerability exists when processing malformed playlist files, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Zinf Malformed Playlist File Remote Buffer Overflow	Medium	Bugtraq, September 24, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apache Software Foundation Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.50	A remote Denial of Service vulnerability exists in Apache 2 mod_ssl during SSL connections. Apache: http://nagoya.apache.org/bugzilla/show_bug.cgi?id=29964 RedHat:http://rhn.redhat.com/errata/RHSA-2004-349.html SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/**	Apache mod_ssl Denial of Service CVE Name: CAN-2004-0748	Low	SecurityFocus, September 6, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:096, September 15, 2004 Gentoo Linux Security Advisory, GLSA 200409-21, September 16, 2004

	We are not aware of any exploits for this vulnerability.			Trustix Secure Linux Security Advisory,TSLSA-2004-0047, September 16, 2004 **Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004** **Fedora Update Notification, FEDORA-2004-313, September 23, 2004**
Apache Software Foundation Apache 2.0.50	A remote Denial of Service vulnerability exists in 'char_buffer_read()' when using a RewriteRule to reverse proxy SSL connections. Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126 SuSE: ftp://ftp.suse.com/pub/suse/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-463.html Gentoo: http://security.gentoo.org/glsa/glsa-200409-21.xml Trustix: http://www.trustix.org/errata/2004/0047/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required; however, Proofs of Concept exploits have been published.	Apache mod_ssl Remote Denial of Service CVE Name: CAN-2004-0751	Low	SecurityTracker Alert ID, 1011213, September 10, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:096, September 15, 2004 RedHat Security Advisory, RHSA-2004:463-09, September 15, 2004 Gentoo Linux Security Advisory GLSA 200409-21, September 16, 2004 Trustix Secure Linux Security Advisory , TSLSA-2004-0047, September 16, 2004 **Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004** **Fedora Update Notification, FEDORA-2004-313, September 23, 2004**
Apache Software Foundation Apache 2.0.51	A vulnerability exists in the merging of the 'Satisfy' directive, which could let a remote malicious user obtain access to restricted resources. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-33.xml Trustix: http://http.trustix.org/pub/trustix/updates/ There is no exploit code required.	Apache Satisfy Directive Access Control Bypass CVE Name: CAN-2004-0811	Medium	SecurityFocus, September 24, 2004
Charles Cazabon getmail 4.0.0b10, 4.0-4.0.13, 4.1-4.1.5; Gentoo Linux 1.4	A vulnerability exists due to insufficient validation of symbolic links when creating users' mail boxes and subdirectories, which could let a malicious user obtain elevated privileges. Upgrades available at: http://www.qcc.ca/~charlesc/software/getmail-4/old-versions/getmail-4.2.0.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-32.xml There is no exploit code required.	Getmail Privilege Escalation	Medium	Secunia Advisory, SA12594, September 20, 2004
Concurrent Versions Systems (CVS) 1.11	A vulnerability exists in Concurrent Versions System (CVS) in which a malicious user can exploit to determine the existence and permissions of arbitrary files and directories. The problem is caused due to an undocumented switch to the "history"	CVS Undocumented Flag Information	Low	iDEFENSE Security Advisory 08.16.04

	command implemented in "src/history.c". Using the "-X" switch and supplying an arbitrary filename, CVS will try to access the specified file and returns various information depending on whether the file exists and can be accessed. Upgrade to version 1.11.17 or 1.12.9 available at: https://www.cvshome.org/ **FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:14/cvs.patch** A Proof of Concept exploit has been published.	Disclosure CVE Name: CAN-2004-0778		**FreeBSD Security Advisory, FreeBSD-SA-04:14, September 20, 2004**
CVS Caldera Conectiva Debian Fedora Gentoo Immunix Mandrake OpenBSD OpenPKG RedHat SGI Slackware SuSE CVS 1.10.7, 1.10.8, 1.11-1.11.6, 1.11.10, 1.11.11, 1.11.14-1.11.16, 1.12.1, 1.12.2, 1.12.5, 1.12.7, 1.12.8; Gentoo Linux 1.4; OpenBSD –current, 3.4, 3.5; OpenPKG Current, 1.3, 2.0	Multiple vulnerabilities exist: a null-termination vulnerability exists regarding 'Entry' lines that was introduced by a previous CVS security patch, which could let a remote malicious user execute arbitrary code; a 'double free' vulnerability exists in the 'Arguments 'command, which could let a remote malicious user execute arbitrary code; a format string vulnerability exists in the processing of the CVS wrapper file, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the handling of the 'Max-dotdot' CVS protocol command, which could let a remote malicious user cause a Denial of Service; a vulnerability exists in the 'serve_notify()' function when handling empty data lines, which could let a remote malicious user execute arbitrary code; several errors exist when reading configuration files containing empty lines from CVSROOT, which could let a remote malicious user cause a Denial of Service; and various integer multiplication overflow vulnerabilities exist, which could let a remote malicious user execute arbitrary code. CVS: https://ccvs.cvshome.org/files/documents/19/194/cvs-1.11.17.tar.gz Debian:http://security.debian.org/pool/updates/main/c/cvs/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1 Gentoo: http://security.gentoo.org/glsa/glsa-200406-06.xml Mandrake: http://www.mandrakesoft.com/security/advisories OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ OpenPKG: ftp://ftp.openpkg.org/release RedHat: http://rhn.redhat.com/errata/RHSA-2004-233.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ SuSE: ftp://ftp.suse.com/pub/suse/ **FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:14/cvs.patch** **A Proof of Concept exploit script has been published.**	CVS Multiple Vulnerabilities CVE Names: CAN-2004-0418, CAN-2004-0417, CAN-2004-0416, CAN-2004-0414	Low/ High (Low if a DoS; and High if arbitrary code can be executed)	Debian Security Advisories, DSA 517-1 & 519-1, June 10 & 15, 2004 Fedora Update Notifications, FEDORA-2004-169 & 170, June 11, 2004 Gentoo Linux Security Advisory, GLSA 200406-06, June 10, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:058, June 9, 2004 OpenPKG Security Advisory , OpenPKG-SA-2004.027, June 11, 2004 RedHat Security Advisory, RHSA-2004:233-07, June 9, 2004 SGI Security Advisories, 20040604-01-U & 20040605-01-U, June 21, 2004 SUSE Security Announcement, SuSE-SA:2004:015, June 9, 2004 **FreeBSD Security Advisory, FreeBSD-SA-04:14, September 20, 2004**
fprobe.sourceforge.net fprobe 1.x	A vulnerability exists in 'fprobe.c' in the 'change user' feature. The impact was not specified. Update available at: http://sourceforge.net/project/showfiles.php?group_id=63535 We are not aware of any exploits for this vulnerability.	fprobe Flaw in 'Change User' Feature	Not Specified	SecurityTracker Alert ID, 1011417, September 26, 2004
FreeRADIUS Server Project FreeRADIUS 0.2-0.5, 0.8, 0.8.1, 0.9-0.9.3. 1.0	A remote Denial of Service vulnerability exists in 'radius.c' and 'eap_tls.c' due to a failure to handle malformed packets. Upgrades available at: ftp://ftp.freeradius.org/pub/radius/freeradius-1.0.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-29.xml There is no exploit code required.	FreeRADIUS Access-Request Denial of Service	Low	Gentoo Linux Security Advisory, GLSA 200409-29, September 22, 2004
GNU a2ps 4.13	A vulnerability exists in filenames due to insufficient validation of shell escape characters, which could let a malicious user execute arbitrary commands. FreeBSD: http://www.freebsd.org/cgi/cvsweb.cgi/~checkout~/ports/print/a2ps-letter/files/patch-select.c?rev=1.1&content-type=text/plain	GNU a2ps Command Injection	High	Securiteam, August 29, 2004 SUSE Security Announcement, SUSE-

	SuSE: ftp://ftp.suse.com/pub/suse/ **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57649-1&searchclause=** There is no exploit code required; however, a Proof of Concept exploit has been published.			SA:2004:034, September 17, 2004 **Sun(sm) Alert Notification, 57649, September 23, 2004**
IBM AIX 5L Version 5.2 on pSeries, 5.3 on pSeries, 5.2, 5.3 on an i5/OS (iSeries) partition, Tivoli System Automation (TSA) for Linux 1.1, Multiplatforms 1.2, Cluster Systems Management (CSM) for Linux Version 1.4, (version 1.4 and greater), Hardware Management Console (HMC) for pSeries Version 3, , General Parallel File System (GPFS) Version 2 Release 2 on Linux for xSeries and Linux for pSeries	An input validation vulnerability exists in the Reliable Scalable Cluster Technology (RSCT) system 'ctstrtcasd,' which could let a malicious user create or corrupt arbitrary files. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	IBM Reliable Scalable Cluster Technology (RSCT) File Corruption CVE Name: CAN-2004-0828	Medium	iDEFENSE Security Advisory, September 27, 2004
Jabberd project jabberd 1.4-1.4.3, jadc2s 0.6-0.9	A remote Denial of Service vulnerability exists due to an error in the parsing of XML. Patches available at: http://devel.amessage.info/jabberd14/ http://devel.amessage.info/jadc2s/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-31.xml There is no exploit code required; however, a Proof of Concept exploit has been published.	jabberd XML Parsing Remote Denial of Service	Low	Secunia Advisory, SA12636, September 23, 2004
Jamie Cameron Usermin 1.0 80, 1.0 70, 1.0 60, 1.0 51, 1.0 40, 1.0 30, 1.0 20, 1.0 10, 1.0 00, Webmin1.0 90, 1.0 80, 1.0 70, 1.0 60, 1.0 50, 1.0 20, 1.0 00, 1.100, 1.110, 1.121, 1.130, 1.140, 1.150	A vulnerability exists due to the insecure creation of temporary files during installation, which could let a malicious user obtain sensitive information. Usermin: http://freshmeat.net/redir/usermin/28573/url_tgz/usermin-1.090.tar.gz Webmin: http://prdownloads.sourceforge.net/webadmin/webmin-1.160.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-15.xml Debian: http://security.debian.org/pool/updates/main/w/webmin/ **Mandrake: http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.	Webmin / Usermin Insecure Temporary File CVE Name: CAN-2004-0559	Medium	SecurityFocus, September 10, 2004 Debian Security Advisory, DSA 544-1, September 14, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:101, September 22, 2004**
LaTeX2rtf LaTeX2rtf 1.9.15	A buffer overflow vulnerability exists in 'expandmacro()' when copying user-supplied data due to insufficient bounds checks, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	LaTeX2rtf Remote Buffer Overflow	High	SecurityTracker Alert ID, 1011367, September 21, 2004
mpg123.de mpg123 0.x	A buffer overflow vulnerability exists in the 'do_layer2()' function, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200409-20.xml **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **An exploit script has been published.**	mpg123 'do_layer2() Function' Remote Buffer Overflow	High	Securiteam, September 7, 2004 Gentoo Linux Security Advisory, GLSA 200409-20, September 16, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:100, September 22, 2004**
Multiple Vendors Apache Software Foundation Apache	A remote Denial of Service vulnerability exists in the Apache mod_dav module when an authorized malicious user submits a specific sequence of LOCK requests. Update available at: http://httpd.apache.org/	Apache mod_dav Remote Denial of Service	Low	SecurityTracker Alert ID, 1011248, September 14,

2.0.50 & prior; Gentoo Linux 1.4; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml RedHat: ftp://updates.redhat.com/enterprise Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required; however, Proof of Concept exploit has been published.	CVE Name: CAN-2004-0809		2004 **Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004** **Fedora Update Notification, FEDORA-2004-313, September 23, 2004**
Multiple Vendors Apache Software Foundation Apache 2.0.50 & prior; Gentoo Linux 1.4; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core1&2; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1; Turbolinux Turbolinux Desktop 10.0	A buffer overflow vulnerability exists in the apr-util library's IPv6 URI parsing functionality due to insufficient validation, which could let a remote malicious user execute arbitrary code. *Note: On Linux based Unix variants this issue can only be exploited to trigger a Denial of Service condition.* Patch available at: http://www.apache.org/dist/httpd/patches/apply_to_2.0.50/CAN-2004-0747.patch Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Redhat: http://rhn.redhat.com/errata/RHSA-2004-463.html http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ TurboLinxux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** We are not aware of any exploits for this vulnerability.	Apache Web Server Remote IPv6 Buffer Overflow CVE Name: CAN-2004-0786	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 16, 2004 **Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004** **Fedora Update Notifications, FEDORA-2004-307 & 308, September 16, 2004**
Multiple Vendors Apache Software Foundation Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.50; Gentoo Linux 1.4; MandrakeSoft Linux Mandrake 9.2, amd64,10.0, AMD64; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1; Turbolinux Turbolinux Desktop 10.0	A buffer overflow vulnerability exists in the 'ap_resolve_env()' function in 'server/util.c' due to insufficient validation, which could let a remote malicious user execute arbitrary code. Apache: Upgrade available at: http://www.apache.org/dist/httpd/httpd-2.0.51.tar.gz Patch available at: http://www.apache.org/dist/httpd/patches/apply_to_2.0.50/CAN-2004-0747.patch Gentoo:http://security.gentoo.org/glsa/glsa-200409-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/enterprise/3WS/en/os/SRPMS/httpd-2.0.46-40.ent.src.rpm SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ TurboLinxux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** We are not aware of any exploits for this vulnerability.	Apache Web Server Configuration File Buffer Overflow CVE Name: CAN-2004-0747	High	SITIC Vulnerability Advisory, September 15, 2004 US-CERT Vulnerability Note VU#481998, September 17, 2004 **Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004** **Fedora Update Notification, FEDORA-2004-313, September 23, 2004**
Multiple Vendors Easy Software Products CUPS 1.1.14-1.1.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A Denial of Service vulnerability exists in 'scheduler/dirsvc.c' due to insufficient validation of UDP datagrams. Update available at: http://www.cups.org/software.php Debian: http://security.debian.org/pool/updates/main/c/cupsys/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **ALTLinux: http://altlinux.com/index.php?module=sisyphus&package=cups**	CUPS Browsing Denial of Service CVE Name: CAN-2004-0558	Low	SecurityTracker Alert ID, 1011283, September 15, 2004 **ALTLinux Advisory, September 17, 2004** **Gentoo Linux Security Advisory GLSA 200409-25, September 20, 2004**

	Gentoo: http://security.gentoo.org/glsa/glsa-200409-25.xml **Slackware: ftp://ftp.slackware.com/pub/slackware/** A Proof of Concept exploit has been published.			**Slackware Security Advisory, SSA:2004-266-01, September 23, 2004**
Multiple Vendors Enlightenment Imlib2 1.0-1.0.5, 1.1, 1.1.1; ImageMagick ImageMagick 5.4.3, 5.4.4 .5, 5.4.8 .2-1.1.0 , 5.5.3 .2-1.2.0, 5.5.6 .0-2003040, 5.5.7,6.0.2; Imlib Imlib 1.9-1.9.14	Multiple buffer overflow vulnerabilities exist in the Iimlib/Imlib2 libraries when handling malformed bitmap images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Imlib: http://cvs.sourceforge.net/viewcvs.py/enlightenment/e17/ ImageMagick: http://www.imagemagick.org/www/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200409-12.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-465.html SuSE:ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57648-1&searchclause=** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57645-1&searchclause=** We are not aware of any exploits for this vulnerability.	IMLib/IMLib2 Multiple BMP Image Decoding Buffer Overflows CVE Names: CAN-2004-0817, CAN-2004-0802	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 1, 2004 Gentoo Linux Security Advisory, GLSA 200409-12, September 8, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:089, September 8, 2004 Fedora Update Notifications, FEDORA-2004-300 &301, September 9, 2004 Turbolinux Security Advisory, TLSA-2004-27, September 15, 2004 RedHat Security Advisory, RHSA-2004:465-08, September 15, 2004 Debian Security Advisories, DSA 547-1 & 548-1, September 16, 2004 **Conectiva Linux Security Announcement, CLA-2004:870, September 28, 2004** **Sun(sm) Alert Notifications, 57645 & 57648, September 20, 2004**
Multiple Vendors Gentoo Linux 1.4; RedHat Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1, Desktop 3.0, t Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, 2.1 IA64, 2.1, AS 3, AS 2.1 IA64, AS 2.1' Trolltech Qt 3.0, 3.0.5, 3.1, 3.1.1, 3.1.2, 3.2.1, 3.2.3, 3.3 .0, 3.3.1, 3.3.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'read_dib()' function when handling 8-bit RLE encoded BMP files, which could let a malicious user execute arbitrary code; and buffer overflow vulnerabilities exist in the in the XPM, GIF, and JPEG image file handlers, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/q/qt-copy/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-20.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kde/qt-3.1.2-i486-4.tgz SuSE: ftp://ftp.suse.com/pub/suse/i386/update Trolltech Upgrade: http://www.trolltech.com/download/index.html TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57637-1&searchclause=security	QT Image File Buffer Overflows CVE Names: CAN-2004-0691, CAN-2004-0692, CAN-2004-0693	High	Secunia Advisory, SA12325, August 10, 2004 Sun Alert ID: 57637, September 3, 2004 **Conectiva Linux Security Announcement, CLA-2004:866, September 22, 2004**

	Conectiva: ftp://atualizacoes.conectiva.com.br/ Proof of Concept exploit has been published.			
Multiple Vendors GNU Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; GNOME gdk-pixbug 0.22 & prior; GTK GTK+ 2.0.2, 2.0.6, 2.2.1, 2.2.3, 2.2.4; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64; RedHat Advanced Workstation for the Itanium Processor 2.1, IA64, Desktop 3.0, Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, ES 2.1 IA64, ES 2.1, AS 3, AS 2.1 IA64, AS 2.1, RedHat Fedora Core1&2; SuSE. Linux 8.1, 8.2, 9.0, x86_64, 9.1, Desktop 1.0, Enterprise Server 9, 8	Multiple vulnerabilities exist: a vulnerability exists when decoding BMP images, which could let a remote malicious user cause a Denial of Service; a vulnerability exists when decoding XPM images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability exists when attempting to decode ICO images, which could let a remote malicious user cause a Denial of Service. Debian: http://security.debian.org/pool/updates/main/g/gdk-pixbuf/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SuSE: ftp://ftp.suse.com/pub/suse/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-28.xml** We are not aware of any exploits for this vulnerability.	gdk-pixbug BMP, ICO, and XPM Image Processing Errors CVE Names: CAN-2004-0753, CAN-2004-0782, CAN-2004-0783, CAN-2004-0788	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011285, September 17, 2004 **Gentoo Linux Security Advisory, GLSA 200409-28, September 21, 2004**
Multiple Vendors Linux Kernel 2.6.x, 2.4.x	A vulnerability exists in the 'SG_IO' functionality in 'ide-cd,' which could let a malicious user bypass certain security restrictions. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Linux Kernel ide-cd SG_IO Security Restriction Bypass CVE Name: CAN-2004-0813	Medium	Secunia Advisory, SA12498, September 28, 2004
Multiple Vendors LinuxPrinting.org Foomatic-Filters 3.03.0.2, 3.1; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A vulnerability exists in the foomatic-rip print filter due to insufficient validation of command-lines and environment variables, which could let a remote malicious user execute arbitrary commands. Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** **Gentoo: http://security.gentoo.org/glsa/glsa-200409-24.xml** We are not aware of any exploits for this vulnerability.	LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution CVE Name: CAN-2004-0801	High	Secunia Advisory, SA12557, September 16, 2004 **Fedora Update Notification, FEDORA-2004-303, September 21, 2004** **Gentoo Linux Security Advisory, GLSA 200409-24, September 17, 2004**
Multiple Vendors Luke Mewburn lukemftp 1.5, TNFTPD 20031217; NetBSD Current, 1.3-1.3.3, 1.4 x86, 1.4, SPARC, arm32, Alpha, 1.4.1 x86, 1.4.1, SPARC, sh3, arm32, Alpha, 1.4.2 x86, 1,4.2, SPARC, arm32, Alpha, 1.4.3, 1.5 x86, 1.5, sh3, 1.5.1-1.5.3, 1.6, beta, 1.6-1.6.2, 2.0	Several vulnerabilities exist in the out-of-band signal handling code due to race condition errors, which could let a remote malicious user obtain superuser privileges. Luke Mewburn Upgrade: ftp://ftp.netbsd.org/pub/NetBSD/misc/tnftp/tnftpd-20040810.tar.gz Apple: http://wsidecar.apple.com/cgi-bin/ **Debian: http://security.debian.org/pool/updates/main/l/lukemftpd/** **Gentoo: http://security.gentoo.org/glsa/glsa-200409-19.xml** We are not aware of any exploits for this vulnerability.	TNFTPD Multiple Signal Handler Remote Privilege Escalation CVE Name: CAN-2004-0794	High	NetBSD Security Advisory 2004-009, August 17, 2004 Apple Security Update, APPLE-SA-2004-09-07, September 7, 2004 **Debian Security Advisory DSA 551-1, September 21, 2004** **Gentoo Linux Security Advisory, GLSA 200409-19, September 16, 2004**
MySQL.com MySQL prior to 4.1.5	A remote buffer overflow vulnerability exists in ' libmysqlclient.' The impact was not specified. Update available at: http://dev.mysql.com/downloads/mysql/4.1.html We are not aware of any exploits for this vulnerability.	MySQL libmysqlclient Buffer Overflow	Not Specified	SecurityTracker Alert ID, 1011408, September 24, 2004

NoisyB flc 1.0.4 & prior	A buffer overflow vulnerability exists in 'flc.c,' which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	flc Command Line Buffer Overflow	High	SecurityTracker Alert ID, 1011409, September 25, 2004
OpenBSD OpenBSD 3.2, 3.4, 3.5	A vulnerability exists in the 'login_radius(8') RADIUS authentication implementation, which could let a remote malicious user obtain unauthorized access. Patches available at: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/ There is no exploit code required.	OpenBSD login_radius() Authentication Bypass	Medium	SecurityFocus, September 21, 2004
PHP Arena paFileDB 3.1 Final	An input validation vulnerability exists in the 'id' field due to insufficient filtering of HTML code, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	paFileDB 'file' Input Validation	High	Bugtraq, September 25, 2004
phpMyWebhosting version 0.3.4	Multiple input validation vulnerabilities exist in phpMyWebhosting that allow malicious users to gain elevated privileges as well as enter to the product's management system without knowing the administrative password. phpMyWebhosting does not verifying incoming user input for arbitrary SQL statements. If magic_quotes_gpc is disabled in PHP settings, a remote malicious user can cause SQL injection vulnerability in phpMyWebhosting. **Patch available at: https://sourceforge.net/project/showfiles.php?group_id=85616** We are not aware of any exploits for this vulnerability.	phpMyWebhosting SQL Injection Vulnerabilities	High	SecuriTeam, August 16, 2004 **Bugtraq, September 20, 2004**
RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3	A vulnerability exists in redhat-config-nfs because incorrect permissions may be set in '/etc/exports' when exporting to multiple hosts, which could let a remote malicious user obtain sensitive information. Updates available at: ftp://updates.redhat.com/enterprise There is no exploit code required.	Red Hat redhat-config-nfs Exported Shares Configuration CVE Name: CAN-2004-0750	Medium	Red Hat Security Advisory, RHSA-2004:434-01, September 23, 2004
Samba.org Samba version 3.0 - 3.0.6	Several vulnerabilities exist: a remote Denial of Service vulnerability exists in the 'process_logon_packet()' function due to insufficient validation of 'SAM_UAS_CHANGE' request packets; and a remote Denial of Service vulnerability exists when a malicious user submits a malformed packet to a target 'smbd' server. Updates available at: http://samba.org/samba/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ **RedHat: http://rhn.redhat.com/errata/RHSA-2004-467.html** We are not aware of any exploits for this vulnerability.	Samba Remote Denials of Service CVE Names: CAN-2004-0807, CAN-2004-0808	Low	Securiteam, September 14, 2004 Gentoo Linux Security Advisory, GLSA 200409-16, September 13, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:092, September 13, 2004 Trustix Secure Linux Bugfix Advisory, TSL-2004-0046, September 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.040, September 15, 2004 SUSE Security Announcement, SUSE-SA:2004:034, September 17, 2004 **RedHat Security Advisory, RHSA-2004:467-08, September 23, 2004**
Sendmail Consortium Sendmail 8.12.3, 8.13.1	A vulnerability exists in sendmail as distributed with Debian Linux, which could let a remote malicious user send SPAM via the system.	Sendmail 'sasl-bin' on Debian Linux	Medium	Debian Security Advisory, DSA 554-1,

	Debian: http://security.debian.org/pool/updates/main/s/sendmail/ We are not aware of any exploits for this vulnerability.	CVE Name: CAN-2004-0833		September 27, 2004
SpamAssassin.org SpamAssassin prior to 2.64	A Denial of Service vulnerability exists in SpamAssassin. A a remote user can send an e-mail message with specially crafted headers to cause a Denial of Service attack against the SpamAssassin service. Update to version (2.64), available at: http://old.spamassassin.org/released/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** We are not aware of any exploits for this vulnerability.	SpamAssassin Remote Denial of Service CVE Name: CAN-2004-0796	Low	SecurityTracker: 1010903, August 10, 2004 Mandrake Security Advisory, MDKSA-2004:084, August 19, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.041, September 15, 2004 Conectiva Linux Security Announcement, CLA-2004:867, September 22, 2004
Subversion Subversion 1.0-1.0.7, 1.1 .0 rc1-rc3	A vulnerability exists in the 'mod_authz_svn' module due to insufficient restricted access to metadata on unreadable paths, which could let a remote malicious user obtain sensitive information. Update available at: http://subversion.tigris.org/tarballs/subversion-1.0.8.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ There is no exploit code required.	Subversion Mod_Authz_Svn Metadata Information Disclosure CVE Name: CAN-2004-0749	Medium	SecurityTracker Alert ID, 1011390, September 23, 2004
tutos.org Tutos 1.1 .20040414	Multiple vulnerabilities exist: a vulnerability exists in '/file/file_overview.php' due to insufficient sanitization of the 'link_id' parameter, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists in the address book due to insufficient sanitization of the search field and in 'app_new.php' due to insufficient sanitization of the 't- parameter, which could let a remote malicious user execute arbitrary code. Update available at: http://www.tutos.org/download/ Proofs of Concept exploits have been published.	Tutos Multiple Remote Input Validation Vulnerabilities	High	Secunia Advisory, SA12606, September 21, 2004
xinehq.de xine 0.5.2 - 0.5.x; 0.9.x; 1-alpha.x; 1-beta.x; 1-rc - 1-rc5	Multiple vulnerabilities exist: a buffer overflow in the DVD subpicture component, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the VideoCD functionality when reading ISO disk labels, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists when handling text subtitles, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/xine/xine-lib-1-rc6a.tar.gz?download **Gentoo: http://security.gentoo.org/glsa/glsa-200409-30.xml** We are not aware of any exploits for this vulnerability.	Xine-lib Multiple Buffer Overflows	High	Secunia Advisory, SA12602 September 20, 2004 **Gentoo Linux Security Advisory, GLSA 200409-30, September 22, 2004**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
@lexPHPteam @lex Guestbook	An input validation vulnerability exists in @lex Guestbook, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	@lex Guestbook Include File Remote Code Execution	High	SecurityTracker Alert ID, 1011432, September 28, 2004
AllWebScripts MySQLGuest	A Cross-Site Scripting vulnerability exists in the 'AWSguest.php' script due to insufficient filtering of HTML code from user-supplied input in the 'Name,' 'Email,' 'Homepage,' and 'Comments' fields, 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.	MySQLGuest Cross-Site Scripting	High	SecurityFocus, September 22, 2004
America Online, Inc.	Several vulnerabilities exist: a vulnerability exists in Groups@AOL due to a flaw in the group invitation feature, which could let a remote authenticated malicious user	Groups@AOL Group	Medium	SecurityTracker Alert ID,

AOL	obtain sensitive information; and a vulnerability exists because multiple invitations can be sent to a single screen name, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit has been published.	Invitation		1011414, September 26, 2004
Baal Systems Baal Smart Forms 3.x	A vulnerability exists in the 'Admin Change Password' page due to insufficient security restrictions, which could let a remote malicious obtain administrative access. Update available at: http://baalsystems.com/portal-software-download.shtml A Proof of Concept exploit has been published.	Baal Smart Forms 'Admin Change Password' Security Restriction	High	Secunia Advisory, SA12649, September 27, 2004
Canon imageRUNNER IR5000i	A vulnerability exists due to a failure to require authorization when printing email messages, which could let a remote malicious user print arbitrary text and potentially cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required.	Canon imageRunner Promiscuous Email Printing	Medium	Bugtraq, September 23, 2004
Inkra Networks 1504GX Virtual Service Switch, VSM 2.1.4.b003, 1518TX Virtual Service Switch, 1519TX Virtual Service Switch, 4000 Virtual Service Switch	A remote Denial of Service vulnerability exists due to a failure to handle exceptional network data. The vendor has released an upgraded version of the VSM firmware. There is no exploit code required.	Inkra Router Virtual Service Switch Remote Denial of Service	Low	SecurityFocus, September 23, 2004
Macromedia JRun 3.0, 3.1, 4.0,	Multiple vulnerabilities exist: a vulnerability exists due to an implementation error in the generation and handling of JSESSIONIDs, which could let a remote malicious user hijack an authenticated user's session; a Cross-Site Scripting vulnerability exists in the JRUN Management Console, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to an URL parsing error, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists in the verbose logging module. Patches available at: http://www.macromedia.com/support/jrun/updaters.html We are not aware of any exploits for these vulnerabilities.	Macromedia JRun Multiple Remote Vulnerabilities	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	Macromedia Security Bulletin, MPSB04-08, September 23, 2004
Macromedia ColdFusion MX 6.0, 6.1, J2EE	Two vulnerabilities exist: a vulnerability exists when a remote malicious user submits a specially crafted request that ends with the ';.cfm' string, which could disclosure sensitive information; and a remote Denial of Service vulnerability exists in the verbose logging module. Updates available at: http://www.macromedia.com/devnet/security/security_zone/mpsb04-09.html We are not aware of any exploits for these vulnerabilities.	Macromedia ColdFusion MX Source Code Disclosure	Low/ Medium (Low if a DoS; Medium if sensitive information can be obtained)	Macromedia Security Bulletin, MPSB04-09, September 23, 2004
Mambo Mambo Open Source 4.5.1 (1.0.9)	Two vulnerabilities exist: a vulnerability exists in '.index.php' due to insufficient verification of the 'filecatid' parameter, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'mosConfig_absolute_path' parameter, which could let a remote malicious user execute arbitrary code. The vendor has issued a fix, available via CVS. Proofs of Concept exploits have been published.	Mambo Server Input Validation	High	SecurityTracker Alert ID, 1011365, September 20, 2004
Motorola WR850G 4.0 3 firmware	A vulnerability exists due to an error in the session handling, which could let a remote malicious user execute arbitrary commands with administrative privileges; and a vulnerability exists which could let a remote malicious user access the 'frame_debug.asp' page to obtain shell access on the system. No workaround or patch available at time of publishing. There is no exploit code required.	Motorola Wireless Router WR850G Authentication Circumvention	High	SecurityTracker Alert ID, 1011413, September 26, 2004
Mozilla.org Mandrakesoft Slackware Mozilla 1.7 and prior; Firefox 0.9 and prior; Thunderbird 0.7 and prior	Multiple vulnerabilities exist in Mozilla, Firefox, and Thunderbird that could allow a malicious user to conduct spoofing attacks, compromise a vulnerable system, or cause a Denial of Service. These vulnerabilities include buffer overflow, input verification, insecure certificate name matching, and out-of-bounds reads. Upgrade to the latest version of Mozilla, Firefox, or Thunderbird available at: http://www.mozilla.org/download.html Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.667659 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:082 RedHat: http://rhn.redhat.com/errata/RHSA-2004-421.html	Mozilla Multiple Vulnerabilities CVE Name: CAN-2004-0757, CAN-2004-0759, CAN-2004-0761 CAN-2004-0765	High	Secunia, SA10856, August 4, 2004 US-CERT Vulnerability Note VU#561022 RedHat Security Advisory, RHSA-2004:421-17, August 4, 2004 SGI Security

	SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-26.xml** We are not aware of any exploits for this vulnerability.			Advisory, 20040802-01-U, August 14, 2004 **Gentoo Linux Security Advisory, GLSA 200409-26, September 20, 2004**
Mozilla.org Mozilla 0.x, 1.0-1.7.x, Firefox 0.x, Thunderbird 0.x; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2	Multiple vulnerabilities exist: buffer overflow vulnerabilities exist in 'nsMsgCompUtils.cpp' when a specially crafted e-mail is forwarded, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient restrictions on script generated events, which could let a remote malicious user obtain sensitive information; a buffer overflow vulnerability exists in the 'nsVCardObj.cpp' file due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'nsPop3Protocol.cpp' due to boundary errors, which could let a remote malicious user execute arbitrary code; a heap overflow vulnerability exists when handling non-ASCII characters in URLs, which could let a remote malicious user execute arbitrary code; multiple integer overflow vulnerabilities exist in the image parsing routines due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a cross-domain scripting vulnerability exists because URI links dragged from one browser window and dropped into another browser window will bypass same-origin policy security checks, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because unsafe scripting operations are permitted, which could let a remote malicious user manipulate information displayed in the security dialog. Updates available at: http://www.mozilla.org/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-26.xml** **Proofs of Concept exploits have been published.**	Mozilla Multiple Remote Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Technical Cyber Security Alert TA04-261A, September 17, 2004 US-CERT Vulnerability Notes VU#414240, VU#847200, VU#808216, VU#125776, VU#327560, VU#651928, VU#460528, VU#113192, September 17, 2004 **Gentoo Linux Security Advisory, GLSA 200409-26, September 20, 2004**
myserverproject.net MyServer 0.7.1	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted HTTP POST request. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	MyServer HTTP POST Request Remote Denial of Service	Low	SP Research Labs Advisory x14, September 27, 2004
PeopleSoft PeopleSoft HRMS 7	A Cross-Site Scripting vulnerability exists in some debugging and utility scripts that are included in the default installation, which could let a remote malicious user execute arbitrary HTML and scriptcode. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	PeopleSoft Human Resources Management System (HRMS) Cross-Site Scripting	High	AUSCERT Advisory, September 28, 2004
phpscheduleit.sourceforge.net phpScheduleIt 1.0 .0RC1	Cross-Site Scripting vulnerabilities exist in the 'Name' and 'Last Name' fields in the new user registration script and the 'Schedule Name' field in the new schedule creation script due to insufficient sanitization of user-supplied HTML input, which could let a remote malicious user execute arbitrary HTML and script code. **Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=95547&package_id=101920&release_id=267509** There is no exploit code required.	phpScheduleIt Cross-Site Scripting	High	Bugtraq, August 31, 2004 **Bugtraq, September 17, 2004**
Symantec Firewall/VPN Appliance 100, 200, 200R, Gateway Security 320, 360, 360R	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user conducts a fast map UDP port scan against all ports on the WAN interface; a vulnerability exists when a UDP port scan is conducted against the WAN interface from a source port of UDP 53, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because the default read/write community string used by the firewall is public, which could let a malicious user alter the firewall's configuration. The vendor has released a fixed firmware version (1.63) available at: ftp://ftp.symantec.com/public/updates/ There is no exploit code required.	Symantec Enterprise Firewall/VPN Appliance Multiple Remote Denials of Service & Configuration Modification	Low	Rigel Kent Security & Advisory Services Inc. Advisory, RK-001-04, September 22, 20024
Symantec ON Command CCM 5.0-5.4	A vulnerability exists due to a design error that provides a number of default usernames and passwords, 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.	ON Command Default Usernames & Passwords	Medium	Bugtraq, September 20, 2004
YaBB YaBB 1 Gold Release, SP 1.3.1, SP 1.3, SP 1.2, SP 1	Multiple vulnerabilities exist: an input validation vulnerability exists in 'Adminedit.pl,' which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists due to the way the 'subject' variable is handled, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.yabbforum.com/downloads.php	YaBB 1 Gold Multiple Input Validation	High	Secunia Advisory, SA12609, September 22, 2004

	There is no exploit code required.			
Yahoo! Yahoo! Store	A vulnerability exists in the Yahoo! Store shopping cart, which could let a remote malicious user modify the price of merchandise being purchased. Information regarding the update can be found at: http://help.yahoo.com/help/us/store/store-44.html A Proof of Concept exploit has been published.	Yahoo! Store Commerce System Price Modification	Medium	SecurityTracker Alert ID, 1011403, September 23, 2004
yahoopops.sourceforge.net YPOPs! 0.x	Several buffer overflow vulnerabilities exist in the POP3 and SMTP services, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	YPOPs! Buffer Overflows	High	Hat-Squad Advisory, September 27, 2004

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 Exploit (Reverse Chronological Order)	Exploit Name	Workaround or Patch Available	Script Description
September 28, 2004	MSjpegExploitByFoToZ.c jfif-expII.sh msJPEGParsingVulnHighT1mes.c J pegOfDeath.c jpegOfDeathv0_6_a.c JPGDownloaderATmaCA.c sacred_jpg.c	Yes	Proofs of Concept exploit scripts for the Microsoft (Graphics Device Interface) GDI+ JPEG handler integer underflow vulnerability.
September 23, 2004	activePostFileUploadPOC.zip activePostDoSPOC.zip	No	Proof of Concept exploits for the multiple remote vulnerabilities in ActivePost Messenger. These issues are due to a failure of the application to validate user-supplied input, a failure of the application to handle exceptional conditions, and a design error that fails to properly secure forum passwords.
September 23, 2004	5NP0L0UE0M.html	Yes	Exploit code for a format string vulnerability found in the 'shar' utility. The exploit was tested on Slackware 9.0.
September 23, 2004	scratch.rar	N/A	Scratch is an advanced protocol destroyer which can find a wide variety of vulnerabilities from a simple packet.
September 23, 2004	weplab-0.1.2-beta.tar.gz	N/A	Weplab is a tool to review the security of WEP encryption in wireless networks.
September 23, 2004	xmpg123.c	Yes	Exploit code for the vulnerability in mpg123 that could permit a remote attacker to execute arbitrary code with the privileges of the mpg123 user.
September 22, 2004	arping-2.04.tar.gz	N/A	Arping is an arp level ping utility which broadcasts a who-has ARP packet on the network and prints answers.
September 22, 2004	raddump-0.2.tar.gz	N/A	raddump interprets captured RADIUS packets to print a timestamp, packet length, and other packet information for each packet.
September 22, 2004	EmuliveVuln.txt	No	Proof of Concept exploit for the Emulive Server4 Commerce Edition Build 7560 denial of service vulnerability and unauthorized administrative access due to insufficient input verification.
September 22, 2004	ms04-028.sh	Yes	Proof of Concept local exploit that creates a JPEG image to test for the buffer overrun vulnerability discovered under Microsoft Windows.
September 22, 2004	mdaemon_imap.c mdaemon_rcpt.c	No	Exploit code for the Alt-N MDaemon multiple remote buffer overflow vulnerabilities. The vulnerabilities are likely due to input validation error.
September 21, 2004	lotr3boom.zip	No	Remote denial of service exploit for Lords of the Realm III versions 1.01 and below.
September 21, 2004	lotr3boom.c	No	Script that exploits the Lords of the Realm III Nickname Remote Denial of Service vulnerability.
September 21, 2004	latex2rtf.c	No	Exploit code for the LaTeX2rtf version 1.9.15 remote buffer overflow vulnerability when handling malformed files. This vulnerability may allow a remote attacker to execute arbitrary code on a vulnerable computer to gain unauthorized access.
September 21, 2004	Proof of Concept	No	Proof of Concept exploit for the Pinnacle Systems ShowCenter web-based interface remote denial of service vulnerability. The issue exists due to a lack of sanity checks performed on the Skin parameter of a ShowCenter script.
September 21, 2004	popmsgboom.c	Yes	Exploit for the LeadMind Pop Messenger remote denial of service vulnerability.
September 20, 2004	cvs_argumentx_exp.c	Yes	Exploit code for the double free heap corruption vulnerability in CVS.
September 20, 2004	Proof of Concept	Yes	Proof of Concept exploit for the ReMOSitory module for Mambo SQL injection vulnerability.
September 20, 2004	zp-exp-telnetd.c	Yes	Exploit code for the boundary condition error in telnet daemons derived from the BSD telnet daemon.
September 20, 2004	Proof of Concept	Yes	Proof of Concept exploit for the vulnerability in the Mozilla 'enablePrivilege' method. It is possible to manipulate dialog contents.
September 20, 2004	Proof of Concept	Yes	Proof of Concept exploit for the vulnerability in Mozilla and Firefox browsers that could allow a remote site to gain access to contents of the client user's clipboard.

[back to top]

Trends

- According to the latest Yankee Group 2004 Enterprise Security Services survey of U.S. enterprises, firewalls and antivirus are the two most highly valued security technologies. (SC Magazine, September 27, 2004)

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Netsky-B	Win32 Worm	Stable	February 2004
6	Mydoom.m	Win32 Worm	Stable	July 2004
7	Mydoom.q	Win32 Worm	Stable	August 2004
8	Bagle-AA	Win32 Worm	Stable	April 2004
9	Netsky-Q	Win32 Worm	Stable	March 2004
10	MyDoom-O	Win32 Worm	Stable	July 2004

Table Updated September 24, 2004

Viruses or Trojans Considered to be a High Level of Threat

- JPEG Vulnerability Exploits - Computer code that takes advantage of a flaw in the way many Microsoft applications process JPEG images has been published on the Internet and could be a precursor to actual attacks on vulnerable PCs. The code was published late last week, only days after Microsoft revealed the "critical" vulnerability and made patches available to fix the problem. Microsoft is urging all customers to immediately install the software updates it made available with Security Bulletin MS04-028: http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx (Computerworld, September 22, 2004)

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
Agent.CE	Backdoor.Win32.Agent.ce	Win32 Worm
BackDoor-CHP	Backdoor.Sokeven Backdoor.Win32.Agent.ce Win32/ProxyBot.A	Trojan
Bloodhound.Exploit.14		Trojan: TIFF File
EXPL_JPGDOWN.A		Trojan: JPEG File
HardFull.A	Trj/HardFull.A	Trojan
HTML.Phishbank.BN	HTML/PWS.Cbank.Trojan Phish-BankFraud.eml	E-mail Phishing Scam
JPGDownloader	Constructor/JPGDownloader MS04-028 Hacktool.JPEGDownload Hacktool.JPEGShell JpegOfDeath	JPEG Exploiter
Malam.B	Trj/Malam.B	Trojan
QHosts-16		Trojan
QHosts-16!hosts		Trojan
Rayl.A	AdClicker-BD W32/Rayl.A.worm Worm.MSN.Elon.a	Win32 Worm
TROJ_CHOSENWAN.A		Trojan: JPEG File
Trojan.Upchan		Trojan
VBS.Themis		VBS Script Worm
W32.Donk.S		Win32 Worm
W32.Korgo.AB		Win32 Worm
W32.Randex.BLD		Win32 Worm
W32.Randin		Win32 Worm
W32.Snone.A		Win32 Worm

W32/Agobot-MX	Backdoor.Agobot.bh	Win32 Worm
W32/Forbot-AG	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Forbot-AJ		Win32 Worm
W32/Forbot-AK		Win32 Worm
W32/Forbot-AN		Win32 Worm
W32/Mexer-E		Win32 Worm
W32/MyDoom-D	I-Worm.MyDoom.gen W32/Evaman.d@MM WORM_EVAMAN.D	Win32 Worm
W32/Myfip-C	Worm.Win32.Myfip.c W32/Myfip.worm	Win32 Worm
W32/Noomy-A	W32.Noomy.A@mm	Win32 Worm
W32/Rbot-KJ	Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-KX	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.h	Win32 Worm
W32/Xbot-C	Sdbot.worm.gen.j	Win32 Worm
W32/Zusha-A	Worm.Win32.Zusha.a WORM_ZUSHA.B	Win32 Worm
W97M.Shore.K		MS Word File
Win32.Reign.Z	Backdoor.Trojan TrojanSpy.Win32.Small.az Uploader-S W32/Bizex.B Win32/Reign.Z.Worm	Trojan
Win32.Revcuss.A	BackDoor-CHN TrojanSpy.Win32.Agent.ad Win32/Revcuss.A.Trojan PWSteal.Revcuss.A	Trojan: Password Stealer
Win32.Revcuss.B	PWS-Bancban.gen.e TrojanSpy.Win32.Banker.dm Win32/Revcuss.D.Trojan	Trojan: Password Stealer
Win32.Revcuss.C	PWSteal.Revcuss.C	Trojan: Password Stealer
WORM_AGOBOT.XI	Backdoor.Agobot.qz Win32/Agobot.TD.Worm	Win32 Worm
WORM_AGOBOT.XJ	Backdoor.Agobot.su W32/Agobot.AJH Win32/Agobot.XU.Worm	Win32 Worm

[back to top]

Last updated