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

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

Bugs, Holes, & Patches

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
3Com 3CServer	Buffer overflow vulnerabilities exist in several FTP commands, 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.	3Com 3CServer FTP Command Buffer Overflows CVE Name: CAN-2005-0419	High	Bugtraq, February 7, 2005

ArGoSoft ArGoSoft Mail Server 1.8.7.3 & prior	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists in attachment handling due to insufficient input validation, which could let a remote malicious user obtain sensitive information; a Directory Traversal vulnerability exists in the '_msgatt.rec' file, which could let a remote malicious user include arbitrary files as a email attachment; and a vulnerability exists due to insufficient sanitization of the 'Folder' parameter in 'msg,' 'delete,' 'folderdelete,' and 'folderadd,' which could let a remote malicious user create/delete arbitrary directories. Update available at: http://www.argosoft.com/mailserver/download.aspx There is no exploit code required.	ArGoSoft Mail Server Directory Traversals CVE Name: CAN-2005-0367	Medium	SIG^2 Vulnerability Research Advisory, February 9,2005
ASPJar Guestbook 1.0	Several vulnerabilities exist: a vulnerability exists in the '/admin/login.asp' script due to insufficient sanitization of the 'User' and 'Password' parameters, which could let a remote malicious user obtain administrative access; and a vulnerability exists in 'delete.asp' due to insufficient authorization, which could let a remote malicious user delete arbitrary messages. No workaround or patch available at time of publishing. There is no exploit code required.	ASPJar Guestbook Input Validation CVE Names: CAN-2005-0423 CAN-2005-0424	Medium/ High (High if administrative access can be obtained)	Bugtraq, February 10, 2005
Computer Associates BrightStor ARCserve 2000 Backup Windows Japanese, ARCServe Backup for NetWare 9.0, 11.1, BrightStor ARCServe Backup for Windows 9.0.1, 11.0, 11.1, Windows 64 bit 9.0.1, 11.0, 11.1, Enterprise Backup 10.0, 10.5, Enterprise Backup for Windows 64 bit 10.5	A buffer overflow vulnerability exists when a specially crafted UDP probe is submitted to the Discovery Service, which could let a remote malicious user execute arbitrary code. Patches available at: http://supportconnect.ca.com/sc/ An exploit script has been published.	BrightStor ARCserve Backup Discovery Service Buffer Overflow CVE Name: CAN-2005-0260	High	iDEFENSE Security Advisory, February 9, 2005
DelphiTurk DelphiTurk FTP 1.0	A vulnerability exists in the 'profile.dat' file due to insecure storage of account information, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	DelphiTurk FTP Information Disclosure CVE Name: CAN-2005-0421	Medium	SecurityTracker Alert, 1013139, February 10, 2005
DelphiTurk CodeBank (KodBank) 3.1 & prior	A vulnerability exist because the registry can be searched to obtain usernames & passwords, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	DelphiTurk CodeBank (KodBank) Elevated Privileges CVE Name: CAN-2005-0422	Medium	SecurityTracker Alert, 1013139, February 10, 2005
F-Secure Anti-Virus 2004, 2005.	A buffer overflow vulnerability exists when processing the ARJ archives, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.f-secure.com/security/fsc-2005-1.shtml Currently we are not aware of any exploits for this vulnerability.	F-Secure ARJ Archive Buffer Overflow CVE Name: CAN-2005-0350	High	ISS X-Force Security Advisory, February 10, 2005
IBM DB2 Universal	A vulnerability exists which could let a malicious user cause a Denial of Service or obtain sensitive information.	IBM DB2 Denial of Service & Information	Low/ Medium (Medium if	SecurityFocus, February 10, 2005

Database for Windows 7.1, 7.2, 8.0, 8.1	Updates available at: http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24008763 Currently we are not aware of any exploits for this vulnerability.	Disclosure	sensitive information can be obtained)	
IBM Websphere Application Server 5.0.2.5-5.0.2.9, 5.1.0.2-5.1.0.5, 5.1.1.1-5.1.1.3	A vulnerability exists because the source code of Java Script pages is disclosed via a specially crafted URL, which could let a remote malicious user obtain sensitive information. Updates available at: ftp://ftp.software.ibm.com/software/websphere/appserv/support/fixes/PQ99537/PQ99537_fix.jar There is no exploit code required.	IBM WebSphere Application Server JSP Engine Source Code Disclosure CVE Name: CAN-2005-0425	Medium	Secunia Advisory, SA14274, February 14, 2005
IBM Websphere Application Server 6.0	A vulnerability exists in the file serving servlet, which could let a remote malicious user obtain sensitive information. Updates available at: ftp://ftp.software.ibm.com/software/websphere/appserv/support/fixes/PK00091/6.0.0.1-WS-WAS-IFPK00091.pak There is no exploit code required.	IBM WebSphere Application Server File Servlet Source Code Disclosure CVE Name: CAN-2005-0425	Medium	Secunia Advisory, SA14274, February 14, 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.** 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 Vulnerability Note VU#283646 **Microsoft Security Bulletin, MS05-004 V1.1, February 15, 2005**
Microsoft Internet Explorer 5.0.1, SP1-SP4, r 5.5, SP1&SP2, 6.0 SP1&SP2	A vulnerability exists when certain mouse events are contained in a HREF tag, which could let a remote malicious user display false information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer HREF Tag Mouse Event	Medium	SecurityFocus, February 14, 2005
Microsoft Internet Explorer 5.5, SP1 & SP2, 6.0, SP1 & SP2	A vulnerability exists if the 'CTRL-d' key combination is pressed to bookmark a website that contains a specially crafted pop-up window, 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.	Microsoft Internet Explorer Favorites List	High	SecurityFocus, February 14, 2005
Microsoft Internet Explorer 6.0 SP1	A remote Denial of Service vulnerability exists when a malformed 'file:' URI is processed. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer Malformed 'File:' URI Denial of Service	Low	SecurityFocus, February 15, 2005

Microsoft Office XP SP2 & SP3, Project 2002, Visio 2002, Works Suite 2002, 2003, 2004	A buffer overflow vulnerability exists due to a boundary error in the process that passes URL file locations to Office, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-005.mspx **V1.1: Bulletin updated to clarify prerequisites under Visio 2002 Update Information.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Office URL File Location Handling Buffer Overflow CVE Name: CAN-2004-0848	High	Microsoft Security Bulletin, MS05-005, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#416001 **Microsoft Security Bulletin, MS05-005 V1.1, February 15, 2005**
Microsoft Windows SharePoint Services for Windows Server 2003, SharePoint Team Services from Microsoft	A Cross-Site Scripting and spoofing vulnerability exists due to insufficient validation of input provided to a HTML redirection query before returning it to a user's browser, which could let a remote malicious user execute arbitrary HTML and script code and spoof web browser content. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-006.mspx **V1.1: Bulletin updated to document information about other software that may include the affected software.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows SharePoint Services Cross-Site Scripting & Spoofing CVE Name: CAN-2005-0049	High	Microsoft Security Bulletin, MS05-006, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#340409 **Microsoft Security Bulletin, MS05-006 V1.1, February 15, 2005**
Microsoft Windows Media Player 9 Series, Windows Messenger 5.0, MSN Messenger 6.1, 6.2	Several vulnerabilities exist: a vulnerability exists in Media Player due to a failure to properly handle PNG files that contain excessive width or height values, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the Windows and MSN Messenger due to a failure to properly handle corrupt or malformed PNG files, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-009.mspx **V1.1 Bulletin updated with information on the mandatory upgrade of vulnerable MSN Messenger clients in the caveat section, as well as changes to the Workarounds for PNG Processing Vulnerability in MSN Messenger – CAN-2004-0597** **V1.2: Bulletin updated with correct file version information for Windows Messenger 5.0 update, as well as added Windows Messenger 5.1 to "Non-Affected Software" list.**	Microsoft Media Player & Windows/MSN Messenger PNG Processing CVE Names: CAN-2004-1244 CAN-2004-0597	High	Microsoft Security Bulletin, MS05-009, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#259890 **SecurityFocus,**

	An exploit script has been published for MSN Messenger/Windows Messenger PNG Buffer Overflow vulnerability.			**February 10, 2005** **Microsoft Security Bulletin MS05-009 V1.1, February 11, 2005** **Microsoft Security Bulletin, MS05-009 V1.2, February 15, 2005**
Microsoft Windows 2000 SP 3 & SP4, Windows XP SP1 & SP2, Windows XP 64-Bit Edition SP1 (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	A vulnerability exists in the DHTML Edit ActiveX control, which could let a remote malicious user inject arbitrary scripting code into a different window on the target user's system. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-013.mspx **V1.1: Updated the Caveats section to reflect "None" as there are no caveats associated with this update.** A Proof of Concept exploit has been published.	Microsoft Internet Explorer DHTML Edit Control Script CVE Name: CAN-2004-1319	High	Bugtraq, December 15, 2004 Microsoft Security Bulletin, MS05-013, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#356600 **Microsoft Security Bulletin, MS05-013 V1.1, February 15, 2005**
Microsoft Windows 2000 SP3 & SP4, Windows XP SP1 & SP2, Windows XP 64-Bit Edition SP1, (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	A buffer overflow vulnerability exists in the Hyperlink Object Library when handling hyperlinks, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-015.mspx **V1.1: Mitigating factor for ISA 2004 updated.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Hyperlink Object Library Buffer Overflow CVE Name: CAN-2005-0057	High	Microsoft Security Bulletin, MS05-015, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#820427 **Microsoft Security Bulletin, MS05-015 V1.1, February 15, 2005**

Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Server, Windows 2000 Professional, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Windows Server 2003 Datacenter Edition, Windows 98, Windows 98 SE, Windows ME; Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, 2.0, Avaya S3400 Message Application Server Avaya S8100 Media Servers	A Shell vulnerability and Program Group vulnerability exists in Microsoft Windows. These vulnerabilities could allow remote code execution. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx Bulletin updated to reduce the scope of a documented workaround to only support Windows XP, Windows XP Service Pack 1, and Windows Server 2003. Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Advisories are located at the following locations: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() **V1.2 Bulletin "Caveats" section updated to reflect the availability of Microsoft Knowledge Base Article 891534 as a known issue with this security update on Windows NT Server 4.0 Terminal Server Edition Service Pack 6. This bulletin has also been updated to document that this security update does not replace MS04-024 as was originally described in the bulletin.** We are not aware of any exploits for these vulnerabilities.	Microsoft Windows Shell Remote Code Execution CVE Names: CAN-2004-0214 CAN-2004-0572	High	Microsoft Security Bulletin MS04-037 v1.1, October 25, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 US-CERT Vulnerability Note VU#543864, October 15, 2004 SecurityFocus, October 26, 2004 US-CERT Vulnerability Note, VU#616200, November 23, 2004 **Microsoft Security Bulletin MS04-037 Ver. 1.2, February 15, 2006**
Microsoft Windows (XP SP2 is not affected)	A Denial of Service vulnerability exists in the parsing of ANI files. A remote user can cause the target user's system to hang or crash. A remote user can create a specially crafted Windows animated cursor file (ANI file) that, when loaded by the target user, will cause the target system to crash. The malicious file can be loaded via HTML, for example. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx Bulletin V1.1 (January 20, 2005): Updated CAN reference and added acknowledgment to finder for CAN-2004-1305. **V1.2: Frequently Asked Questions section updated to reflect an additional known attack vector.** Another exploit script has been published.	Microsoft Windows ANI File Parsing Errors CVE Name: CAN-2004-1305	Low	VENUSTECH Security Lab, December 23, 2004 Microsoft Security Bulletin MS05-002, January 11, 2005 US-CERT Vulnerability Notes, VU#177584 & VU#697136, January 11, 2005 SecurityFocus, January 12, 2005 Technical Cyber Security Alert, TA05-012A, January 12, 2005 Microsoft

				Security Bulletin, MS05-002, V1.1, January 20, 2005 PacketStorm, January 31, 2005 **Microsoft Security Bulletin, MS05-002, V1.2, February 15, 2005**
Microsoft Exchange Server 2003, SP1	A vulnerability exists in Microsoft Outlook Web Access due to is insufficient sanitization of URI supplied data, which could let a remote malicious user conduct phishing attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Microsoft Outlook Web Access URI Redirection CVE Name: CAN-2005-0420	Medium	Secunia Advisory, SA14144, February 8, 2005
Multiple Vendors Check Point Software Integrity Client 4.5, Integrity Client 5.0; Zone Labs ZoneAlarm 2.1-2.6, 3.0, 3.1, 3.7 .202, 4.0, 4.5 .538.001, 5.1, ZoneAlarm Pro 2.4, 2.6, 3.0, 3.1, 4.0, 4.5 .538.001, 4.5, 5.0.590.015, 5.1, 5.5 .062, ZoneAlarm Security Suite 5.1, 5.5 .062, 5.5	A Denial of Service vulnerability exists in the 'NtConnectPort' function due to insufficient verification of the 'ServerPortName' argument. Updates available at: http://download.zonelabs.com/bin/free/securityAlert/19.html Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor ZoneAlarm Denial of Service CVE Name: CAN-2005-0114	Low	SecurityTeam, February 13, 2005
RealNetworks RealArcade 1.2.0.994 & prior	Two vulnerabilities exist: a vulnerability exists due to the way RGS files are handled, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in RGP files that contain a specially crafted 'FILENAME' tag, which could let a remote malicious modify system/user information. No workaround or patch available at time of publishing. Exploit scripts have been published.	RealArcade Vulnerabilities CVE Names: CAN-2005-0347 CAN-2005-0348	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert, 1013128, February 9, 2005
Safenet SoftRemote VPN Client	A vulnerability exists because the 'IreIKE.exe' process stores the VPN password in memory, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	SafeNet SoftRemote VPN Client Key Disclosure CVE Name: CAN-2005-0346	Medium	SecurityTracker Alert, 1013134, February 9, 2005
Software602 602LAN SUITE 2004	A vulnerability exists due to improper validation of user-supplied filenames before uploading files as e-mail attachments, which could let a remote malicious user execute arbitrary code. Update available at: http://www.software602.com/download/ Currently we are not aware of any exploits for this vulnerability.	602LAN SUITE Input Validation **CVE Name: CAN-2005-0344**	High	SIG^2 Vulnerability Research Advisory, February 8, 2005
Sybase Adaptive Server Enterprise 11.5 Win, 11.5.1 Win,	A vulnerability exists that affects all versions of Adaptive Server Enterprise prior to 12.0.0.8 ESD#3 and 12.5.3 ESD#1 running on Microsoft Windows platforms. The impact was not specified. Vendor recommendations located at:	Sybase Adaptive Server Enterprise Unspecified	Not Specified	Sybase Security Alert , February 15, 2005

11.9.2 Win, 12.0 Win, 12.0 .0.8 EDS#3, 12.5 Win, 12.5.2, 12.5.3 ESD#1, 12.5.3	http://www.sybase.com/detail/1,6904,1033894,00.html Currently we are not aware of any exploits for this vulnerability.	Vulnerability CVE Name: CAN-2005-0441	

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apple Mac OS X 10.0 3, 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.7, Mac OS X Server 10.0-10.1.5, 10.2-10.2.8, 10.3-10.3.7	A remote Denial of Service vulnerability exists in the AppleFileServer due to a failure to handle integer signedness properly. No workaround or patch available at time of publishing. An exploit script has been published.	Apple Mac OS X AppleFileServer Remote Denial of Service CVE Name: CAN-2005-0340	Low	Bugtraq, February 8,
Apple Mac OS X 10.0 3, 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.7, Mac OS X Server 10.0-10.1.5, 10.2-10.2.8, 10.3-10.3.7	A vulnerability exists in Finder due to the insecure creation of '.DS_Store' files, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. An exploit script has been published.	Apple Mac OS X Finder 'DS_Store' Insecure File Creation CVE Name: CAN-2005-0342	Medium	Bugtraq, February 7,
Apple Safari 1.2.4 v125.12	An input validation vulnerability exists because the HTTP 'Content-type' header value is ignored by the web server, which could let a remote malicious user modify system information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Apple Safari Input Validation **CVE Name: CAN-2005-0341**	Medium	SecurityTracker Alert 1013087, February 5
Brooky CubeCart 2.0.1, 2.0.4	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://www.cubecart.com/site/downloads/ There is no exploit code required; however, a Proof of Concept exploit has been published.	Brooky CubeCart Multiple Vulnerabilities CVE Names: CAN-2005-0442 CAN-2005-0443	Medium/ High (High if arbitrary code can be executed)	Bugtraq, February 14

Caolan McNamara & Dom Lachowicz wvWare version 0.7.4, 0.7.5, 0.7.6 and 1.0.0	A buffer overflow vulnerability exists in the 'strcat()' function call due to the insecure bounds checking, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.abisource.com/bonsai/cvsview2.cgi?diff_mode=context&whitespace_mode=show&root=/cvsroot&subdir=wv&command=DIFF_FRAMESET&root =/cvsroot&file=field.c&rev1=1.19&rev2=1.20 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200407-11.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/w/wv/ **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit has been published.	wvWare Library Buffer Overflow CVE Name: CAN-2004-0645	High	Securiteam, July 11, iDEFENSE Security July 9, 2004 Conectiva Linux Sec Announcement, CLA September 10, 2004 Debian Security Advi 550-1, September 20 Debian Security Advi 579-1, November 1, Conectiva Linux Sec Announcement, CLA December 1, 2004 **Fedora Legacy Upd** **Advisory, FLSA:190** **February 8, 2005**
Computer Associates BrightStor ARCserve 2000, ARCserve Backup 11.x, 9.x, Enterprise Backup 10.x	A vulnerability exists due to a hard-coded backdoor account that contains a common authentication password, which could let a remote malicious user execute arbitrary commands with root privileges. Updates available at: http://supportconnect.ca.com/sc/solcenter/ There is no exploit code required	CA BrightStor ARCserve Backup UniversalAgent Backdoor Account CVE Name: CAN-2005-0349	High	iDEFENSE Security February 10, 2005
Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha, Debian toolchain-source 3.0.3 -1-3.0.3-3, 3.0.4	A vulnerability exists due to the insecure creation of temporary files, which could let a malicious user obtain sensitive information. Update available at: http://security.debian.org/pool/updates/main/t/toolchain-source/toolchain-source_3.0.4-1woody1_all.deb There is no exploit code required.	Debian Toolchain-Source Multiple Insecure Temporary File Creation CVE Name: CAN-2005-0159	Medium	Debian Security Advi 679-1, February 14,
Ethereal Group Ethereal 0.8, 0.8.13-0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.8	Multiple vulnerabilities exist: remote Denial of Service vulnerabilities exist in the COPS, DLSw, DNP, Gnutella, and MMSE dissectors; and a buffer overflow vulnerability exists in the X11 dissector, which could let a remote malicious user execute arbitrary code. Ethereal: http://www.ethereal.com/download.html Debian: http://security.debian.org/pool/updates/main/e/ethereal/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-27.xml 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 these vulnerabilities.	Ethereal Multiple Dissector Vulnerabilities CVE Names: CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert January 21, 2005 **SGI Security Adviso** **20050202-01-U, Feb** **2005**

Gallery Project Gallery 1.4 -pl1&pl2, 1.4, 1.4.1, 1.4.2, 1.4.3 -pl1 & pl2; Gentoo Linux	A Cross-Site Scripting vulnerability exists in several files, including 'view_photo.php,' 'index.php,' and 'init.php' due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=7130 Gentoo: http://security.gentoo.org/glsa/glsa-200411-10.xml Debian: http://security.debian.org/pool/updates/main/g/gallery/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-45.xml It is reported that the fixes released by the vendor to address this issue are ineffective. Gallery 1.4.4-pl2 is still considered vulnerable to cross-site scripting attacks. The fixes are being removed. **Gentoo: The cross-site scripting vulnerability that Gallery 1.4.4-pl5 was intended to fix, did not actually resolve the issue.** There is no exploit code required.	Gallery Cross-Site Scripting **CVE Name: CAN-2004-1106**	High	Gentoo Linux Securit GLSA 200411-10:01, November 6, 2004 Debian Security Advi 642-1, January 17, 2 Gentoo Linux Securit GLSA 200501-45, Ja 2005 SecurityFocus, Febru 2005 **Gentoo Linux Secu Advisory [UPDATE] 200501-45:03, Febru 2005**
Gentoo webmin-1.140.ebuild, 1.150.ebuild, 1.160.ebuild, 1.170-r1.ebuild, 1.170-r2.ebuild	A vulnerability exists in the 'miniserv.users' file due to exposure of the encrypted root password, which could let a remote malicious user obtain sensitive information. Update available at: http://security.gentoo.org/glsa/glsa-200502-12.xml There is no exploit required.	Gentoo Portage-Built Webmin Root Password Disclosure CVE Name: CAN-2005-0427	Medium	Gentoo Linux Securit GLSA 200502-12, Fe 2005
gFTP gFTP 0.1, 0.2, 0.21, 1.0, 1.1-1.13, 2.0-2.0.17	A Directory Traversal vulnerability exists due to insufficient sanitization of input, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.gftp.org/gftp-2.0.18.tar.gz There is no exploit code required.	gFTP Remote Directory Traversal CVE Name: CAN-2005-0372	Medium	SecurityFocus, Febru 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 CVE Name: CAN-2005-0064	High	iDEFENSE Security A January 18, 2005 Conectiva Linux Secu Announcement, CLA January 25, 2005 Mandrakelinux Secu Advisories, MDKSA-2005:016-02 26, 2005 SUSE Security Summ Report, SUSE-SR:20 January 26, 2005 SUSE Security Summ Report, SUSE-SR:20 February 4, 2005 **SGI Security Adviso 20050202-01-U, Feb 2005** **Gentoo Linux Secu Advisory, GLSA 200 February 9, 2005**

	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/** Currently we are not aware of any exploits for this vulnerability.			**Fedora Legacy Upd Advisory, FLSA:235 February 10, 2005** **Trustix Secure Linu Advisory, TSLSA-20 February 11, 2005**
GNU Enscript 1.4, 1.5, 1.6, 1.6.1, 1.6.3, 1.6.4	Multiple vulnerabilities exist in 'src/util.c' and 'src/psgen.c': a vulnerability exists in EPSF pipe support due to insufficient input validation, which could let a malicious user execute arbitrary code; a vulnerability exists due to the way filenames are processed due to insufficient input validation, which could let a malicious user execute arbitrary code; and a Denial of Service vulnerability exists due to several buffer overflows. Debian: http://security.debian.org/pool/updates/main/e/enscript/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/e/enscript/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200502-03.xml** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-039.html** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	GNU Enscript Input Validation CVE Names: CAN-2004-1184 CAN-2004-1185 CAN-2004-1186	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert 1012965, January 21 **RedHat Security Ad RHSA-2005:039-06, 1, 2005** **Gentoo Linux Secur Advisory, GLSA 200 February 2, 2005** **SUSE Security Sum Report, SUSE-SR:20 February 11, 2005** **Mandrakelinux Secu Update Advisory, MDKSA-2005:033, F 11, 2005**

GNU Emacs prior to 21.4.17	A format string vulnerability exists in 'movemail.c,' which could let a remote malicious user execute arbitrary code. Update available at: ftp://ftp.xemacs.org/pub/xemacs/xemacs-21.4 **Debian:** **http://security.debian.org/pool/.../e/emacs20/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/e/emacs21/** Currently we are not aware of any exploits for this vulnerability.	Emacs Format String CVE Name: CAN-2005-0100	High	SecurityTracker Alert February 7, 2005 **Debian Security Ad DSA-670-1 & 671-1, 8, 2005** **Ubuntu Security No USN-76-1, February** **Fedora Update Noti FEDORA-2005-145 & February 14, 2005**
GNU wget 1.9.1	A vulnerability exists which could permit a remote malicious user to create or overwrite files on the target user's system. wget does not properly validate user-supplied input. A remote user can bypass the filtering mechanism if DNS can be modified so that '..' resolves to an IP address. A specially crafted HTTP response can include control characters to overwrite portions of the terminal window. **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** A Proof of Concept exploit script has been published.	GNU wget File Creation & Overwrite CVE Names: CAN-2004-1487 CAN-2004-1488	Medium	SecurityTracker Alert 1012472, December **SUSE Security Sum Report, SUSE-SR:2 February 11, 2005**
GNU Xpdf prior to 3.00pl2	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user. A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html A patch is available: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch KDE: http://www.kde.org/info/security/advisory-20041223-1.txt Gentoo: http://security.gentoo.org/glsa/glsa-200412-24.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ Mandrakesoft (update for koffice): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:165 Mandrakesoft (update for kdegraphics): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:163 Mandrakesoft (update for gpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:162 Mandrakesoft (update for xpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:161 Mandrakesoft (update for tetex):	GNU Xpdf Buffer Overflow in doImage() CVE Name: CAN-2004-1125	High	iDEFENSE Security 12.21.04 KDE Security Adviso December 23, 2004 Mandrakesoft, MDKSA-2004:161,16 166, December 29, 2 Fedora Update Notifi FEDORA-2004-585, 2005 Gentoo Linux Securit GLSA 200501-13, Ja 2005 Conectiva Linux Secu Announcement, CLA January 25, 2005 SUSE Security Sumr Report, SUSE-SR:20 January 26, 2005 Avaya Security Advis ASA-2005-027, Janu 2005 SUSE Security Sumr Report, SUSE-SR:20 February 4, 2005 **SUSE Security Sum Report, SUSE-SR:2 February 4, 2005** **Fedora Legacy Upd Advisory, FLSA:235 February 10, 2005**

	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/** Currently we are not aware of any exploits for this vulnerability.			
Hewlett Packard Company HP-UX B.11.23, HP-UX B.11.11, HP-UX B.11.00	A remote Denial of Service vulnerability exists due to a failure to handle malformed network data. Upgrades available at: http://software.hp.com/ Currently we are not aware of any exploits for this vulnerability.	HP-UX BIND Remote Denial of Service CVE Name: CAN-2005-0364	Low	HP Security Bulletin, HPSBUX01117, Feb 2005
Hewlett Packard HP-UX 11.x	A vulnerability exists in HP-UX, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the debug logging routine of ftpd. This can be exploited to cause a stack-based buffer overflow by sending a specially crafted, overly long command request. Successful exploitation may allow execution of arbitrary code, but requires that the FTP daemon is configured to log debug information (not default setting). Apply patches: http://www.itrc.hp.com/service/patch/mainPage.do **HP:** **http://itrc.hp.com** Currently we are not aware of any exploits for this vulnerability.	Hewlett Packard HP-UX FTP Server Debug Logging Buffer Overflow Vulnerability CVE Name: CAN-2004-1332	High	iDEFENSE Security 12.21.04 **HP Security Bulleti HPSBUX01118, Feb 2005**
IBM AIX 5.1-5.3	A buffer overflow vulnerability exists in 'netpmon' command, which could let a malicious user execute arbitrary code as root. Patches available at: ftp://aix.software.ibm.com/aix/efixes/security/netpmon_efix.tar.Z Currently we are not aware of any exploits for this vulnerability.	IBM AIX 'Netpmon' Command Buffer Overflow CVE Name: CAN-2005-0263	High	iDefense Security Ad February 10, 2005

IBM AIX 5.1-5.3	A buffer overflow vulnerability exists in the 'ipl_varyon' utility due to a failure to copy user-supplied input securely, 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 this vulnerability.	IBM AIX 'IPL_Varyon' Buffer Overflow CVE Name: CAN-2005-0262	High	iDefense Security Ad February 10, 2005
IBM AIX 5.2, 5.3	A vulnerability exists in the 'lspath' command, which could let a malicious user obtain sensitive information. Updates available at: ftp://aix.software.ibm.com/aix/efixes/security/lspath_efix.tar.Z There is no exploit code required.	IBM AIX 'LSPath' Information Disclosure CVE Name: CAN-2005-0261	Medium	IBM Security Advisor February 9, 2005
KAME Project IPsec-Tools 0.3, rc1-rc5, 0.3.1, 0.3.2; KAME Racoon, 20040503, 20040407b, 20040405, 20030711	A vulnerability exists due to an authentication error in the 'eay_check_x509cert()' function when verifying certificates, which could lead to the validation of invalid certificates. Upgrades available at: http://prdownloads.sourceforge.net/ipsec-tools/ipsec-tools-0.3.3.tar.gz?download SGI: http://www.sgi.com/support/security/ Apple: http://download.info.apple.com/Mac_OS_X/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-308.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.10** There is no exploit code required.	KAME Racoon X.509 Certificate Validation CVE Name: CAN-2004-0607	Medium	Bugtraq, June 14, 20 **SCO Security Advis SCOSA-2005.10, Fe 2005**
KAME Project Racoon 20040405, 20030711, Racoon	A remote Denial of Service vulnerability exists due to an error when processing certain malformed IKE messages. Upgrades available at: ftp://ftp.kame.net/pub/kame/snap/kame-20040503-openbsd34-snap.tgz **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.10** Currently we are not aware of any exploits for this vulnerability.	Kame Racoon Remote IKE Message Denial of Service CVE Name: CAN-2004-0392	Low	SecurityFocus, May 6 **SCO Security Advis SCOSA-2005.10, Fe 2005**
KAME Project Racoon Apple Mac OS X 10.2.8, 10.3.3, Mac OS X Server 10.2.8, 10.3.3	A Denial of Service vulnerability exits due to an error when allocating memory for ISAKMP messages. Patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/racoon_patch Apple: http://download.info.apple.com/Mac_OS_X/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-165.html SGI: http://www.sgi.com/support/security/ Mandrake:	Kame Racoon Malformed ISAKMP Packet Denial of Service CVE Name: CAN-2004-0403	Low	Secunia Advisory, SA April 19, 2004 Apple Security Advis APPLE-SA-2004-05- 2004 **SCO Security Advis SCOSA-2005.10, Fe 2005**

	http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200404-17.xml **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.10** Currently we are not aware of any exploits for this vulnerability.			
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 Currently we are not aware of any exploits for this vulnerability.	KDE 'DCOPIDLING' Library CVE Name: CAN-2005-0365	Medium	SecurityFocus, Febru 2005
KDE KDE 3.x, 2.x	A vulnerability exists in kio_ftp, which can be exploited by malicious people to conduct FTP command injection attacks. The vulnerability has been fixed in the CVS repository. Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:160 Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-18.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.suse.com/pub/suse/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-009.html** Currently we are not aware of any exploits for this vulnerability.	KDE kio_ftp FTP Command Injection Vulnerability CVE Name: CAN-2004-1165	Medium	KDE Advisory Bug 95 December 26, 2004 Debian Security Advi 631-1, January 10, 2 Gentoo Linux Securit GLSA 200501-18, Ja 2005 Fedora Update Notifi FEDORA-2005-063 & January 25, 2005 SUSE Security Sumr Report, SUSE-SR:20 February 4, 2005 **RedHat Security Ad RHSA-2005:009-19, 10, 2005**

KDE Konqueror 3.2.2-6	A vulnerability exists which can be exploited by malicious people to spoof the content of websites. A website can inject content into another site's window if the target name of the window is known. This can be exploited by a malicious website to spoof the content of a pop-up window opened on a trusted website. Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:150 Gentoo: http://security.gentoo.org/glsa/ glsa-200412-16.xml SUSE: ftp://ftp.suse.com/pub/suse/ **RedHat: h ttp://rhn.redhat.com/errata/ RHSA-2005-009.html** Currently we are not aware of any exploits for this vulnerability.	KDE Konqueror Window Injection CVE Name: CAN-2004-1158	Medium	Secunia Advisory ID, December 8, 2004 Secunia Advisory ID, December 16, 2004 Mandrakesoft Securi Advisory, MDKSA-20 December 15, 2004 SUSE Security Summ Report, SUSE-SR:20 February 4, 2005 **RedHat Security Ad RHSA-2005:009-19, 10, 2005**
Konversation IRC Client 0.15	Multiple vulnerabilities exist: a vulnerability exists in the 'Server::parseWildcards' function due to insufficient filtering of various parameters, which could let a remote malicious user execute arbitrary code; a vulnerability exists in certain Perl scripts if shell metacharacters in channel names or song names aren't properly quoted, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the Quick Connection dialog because the password is used as the nickname, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://konversation.berlios.de/ Gentoo: http://security.gentoo.org/ glsa/glsa-200501-34.xml **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit required; however, Proofs of Concept exploits have been published.	Konversation IRC Client Multiple Remote Vulnerabilities CVE Names: CAN-2005-0129 CAN-2005-0130 CAN-2005-0131	Medium/ High (High if arbitrary code can be executed)	Bugtraq, January 19, **SUSE Security Sum Report, SUSE-SR:2 February 11, 2005**
Larry Wall Perl 5.8.3	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200412-04.xml Debian: http://security.debian.org/pool/updates/main/p/perl/ OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/ perl-5.8.4-2.1.1.src.rpm **Mandrake:** **http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2005:031** There is no exploit code required.	Perl Insecure Temporary File Creation CVE Name: CAN-2004-0976	Medium	Trustix Secure Linux Advisory, TSL-2004-(September 30, 2004 Ubuntu Security Noti USN-16-1, Novembe Gentoo Linux Securit GLSA 200412-04, De 2004 Debian Security Advi 620-1, December 30, OpenPKG Security A OpenPKG-SA-2005.(January 11, 2005 **MandrakeSoft Secu Advisory, MDKSA-2 February 8, 2005**

LOGICNOW PerlDesk 1.x	An input validation vulnerability exists in the 'kb.cgi' script due to insufficient validation of the 'view' parameter, which could let a remote malicious user execute arbitrary SQL commands. **Upgrades available at:** **http://www.perldesk.com/helpdesk.0.html** **An exploit script has been published.**	PerlDesk 'view' Parameter Input Validation **CVE Name:** **CAN-2005-0343**	High	SecurityTracker Alert, February 7, 2005 **SecurityFocus, Feb 2005**
MIT Kerberos 5 1.3.4	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-24.xml **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-036_RHSA-2005-012.pdf** There is no exploit code required.	MIT Kerberos 5 Insecure Temporary File Creation CVE Name: CAN-2004-0971	Medium	Trustix Secure Linux Advisory, TSL-2004-0 September 30, 2004 Gentoo Linux Securit GLSA 200410-24, Oc 2004 **Avaya Security Adv ASA-2005-036, Febr 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/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** Currently we are not aware of any exploits for this vulnerability.	Kerberos libkadm5srv Heap Overflow CVE Name: CAN-2004-1189	High	SecurityTracker Alert 1012640, December Gentoo GLSA 20050 January 5, 2005 Ubuntu Security Noti USN-58-1, January 1 Conectiva Linux Secu Announcement, CLA January 13, 2005 **Avaya Security Adv ASA-2005-036, Febr 2005**
Multiple Vendors ClamAV 0.51-0.54, 0.60, 0.65, 0.67, 0.68 -1, 0.68, 0.70, 0.80 rc1-rc4, 0.80; MandrakeSoft Corporate Server 3.0 x86_64, 3.0. Linux Mandrake 10.1 X86_64, 10.1	A remote Denial of Service vulnerability exists due to an error in the handling of file information in corrupted ZIP files. Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=300116 Gentoo: http://security.gentoo.org/glsa/glsa-200501-46.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE **Trustix:** **http://www.trustix.org/errata/2005/0003/** Currently we are not aware of any exploits for this vulnerability.	Clam Anti-Virus ClamAV Remote Denial of Service CVE Name: CAN-2005-0133	Low	SecurityFocus, Janua 2005 Mandrakelinux Secur Advisory, MDKSA-20 January 31, 2005 Gentoo Linux Securit GLSA 200501-46, Ja 2005 SUSE Security Sumr Report, SUSE-SR:20 February 4, 2005 **Trustix Secure Linu Advisory, TSLSA-20 February 11, 2005**
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc,	A vulnerability exists in 'iptables.c' and 'ip6tables.c' due to a failure to load the required modules, which could lead to a false sense of security because firewall rules may not always be loaded.	IpTables Initialization Failure	Medium	Debian Security Advi 580-1 , November 1, Mandrakelinux Secu

mipsel, mips, m68k, 0 ia-64, ia-32, hppa, arm, alpha; Linux kernel 2.0.2, 2.4-2.4.26, 2.6-2.6.9	Debian: http://security.debian.org/pool/ updates/main/i/iptables/i Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/ SUSE: ftp.SUSE.com/pub/SUSE TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** **Ubuntu:** **http://security.ubuntu.com /ubuntu/pool/main/i/iptables/** There is no exploit required.	CVE Name: CAN-2004-0986		Advisory, MDKSA-20 November 4, 2004 SUSE Security Sumr Report, SUSE-SR:20 November 30, 2004 Fedora Update Notifi FEDORA-2004-417, 1, 2004 Turbolinux Security A TLSA-2005-10, Janu 2005 **Fedora Legacy Upd** **Advisory, FLSA:225** **February 10, 2005** **Ubuntu Security No** **USN-81-1, February**
Multiple Vendors Exim 4.43 & prior	Multiple vulnerabilities exist that could allow a local user to obtain elevated privileges. There are buffer overflows in the host_aton() function and the spa_base64_to_bits() functions. It may be possible to execute arbitrary code with the privileges of the Exim process. The vendor has issued a fix in the latest snapshot: ftp://ftp.csx.cam.ac.uk/pub/software /email/exim/ Testing/exim-snapshot.tar.gz ftp://ftp.csx.cam.ac.uk/pub/software/ email/exim/Testing/exim-snapshot.tar.gz.sig Also, patches for 4.43 are available at: http://www.exim.org/mail-archives/ exim-announce/2005/msg00000.html Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/e/exim4/ Gentoo: http://security.gentoo.org/glsa/ glsa-200501-23.xml Debian: http://security.debian.org/pool/ updates/main/e/exim/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **An exploit script has been published.**	GNU Exim Buffer Overflows CVE Names: CAN-2005-0021 CAN-2005-0022	High	SecurityTracker Alert 1012771, January 5, Gentoo Linux Securit GLSA 200501-23, Ja 2005 Debian Security Advi 635-1 & 637-1, Janua 13, 2005 SUSE Security Sumr Report, SUSE-SR:20 January 26, 2005 US-CERT Vulnerabil VU#132992, January **SecurityFocus, Feb** **2005**

Multiple Vendors Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4, rc1-rc3; libdbi-perl libdbi-perl 1.21, 1.42	A vulnerability exists libdbi-perl due to the insecure creation of temporary files, which could let a remote malicious user overwrite arbitrary files. Debian: http://security.debian.org/pool/updates/ main/libd/libdbi-perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-069.html Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/libd/libdbi-perl/ **Mandrake:** **http://www.mandrakesoft.com /security/advisories?name=MDKSA-2005:030** **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	Libdbi-perl Insecure Temporary File Creation CVE Name: CAN-2005-0077	Medium	Debian Security Advi 658-1, January 25, 2 Ubuntu Security Noti USN-70-1, January 2 Gentoo Linux Securit GLSA 200501-38, Ja 2005 RedHat Security Adv RHSA-2005:069-08, 1, 2005 **MandrakeSoft Secu Advisory, MDKSA-2 February 8, 2005** **SUSE Security Sum Report, SUSE-SR:2 February 11, 2005**
Multiple Vendors Gentoo Linux; VMWare VMWare Workstation 3.2.1 patch 1, 3.4, 4.0-4.0.2, 4.5.2	A vulnerability exists because binary searches for a shared library is in a world-writeable location, which could let a malicious execute arbitrary code. Updates available at: http://security.gentoo.org/glsa/glsa-200502-18.xml There is no exploit code required.	VMWare Workstation For Linux Shared Library CVE Name: CAN-2005-0444	High	Gentoo Linux Securit GLSA 200502-18, Fe 2005
Multiple Vendors GNU Mailman 1.0, 1.1, 2.0 beta1-beta3, 2.0- 2.0 .3, 2.0.5-2.0 .8, 2.0.1-2.0.14, 2.1 b1, 2.1- 2.1.5; Ubuntu Linux 4.1, ia64, ia32	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists when returning error pages due to insufficient sanitization by 'scripts/driver,' which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists due to a weakness in the automatic password generation algorithm, which could let a remote malicious user brute force automatically generated passwords. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ m/mailman/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-29.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE **Debian:** **http://security.debian.org/pool/ updates/main/m/mailman/** Currently we are not aware of any exploits for these vulnerabilities.	GNU Mailman Multiple Remote Vulnerabilities CVE Names: CAN-2004-1143 CAN-2004-1177	Medium/ High (High if arbitrary code can be executed)	SecurityTracker, Jan 2005 Mandrakelinux Secu Advisory, MDKSA-20 January 25, 2005 SUSE Security Sumr Report, SUSE-SR:20 January 26, 2005 **Debian Security Ad DSA 674-1 & 674-2, 10 & 11, 2005** **SUSE Security Announcement, SUSE-SA:2005:007, 14, 2005**
Multiple Vendors ht//Dig Group ht://Dig 3.1.5 -8, 3.1.5 -7, 3.1.5, 3.1.6, 3.2 .0, 3.2 0b2-0b6; SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, 9.0 x86_64, 9.1, 9.2	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from the 'config' parameter, which could let a remote malicious user execute arbitrary HTML and script code. SuSE: ftp://ftp.suse.com/pub/suse/ **Debian:** **http://security.debian.org/pool/updates/main/h/htdig/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200502-16.xml** There is no exploit code required; however, a Proof of Concept exploit has been published.	ht://Dig Cross-Site Scripting CVE Name: CAN-2005-0085	High	SUSE Security Sumr Report, SUSE-SR:20 February 4, 2005 **Debian Security Ad ,DSA 680-1, Februar** **Gentoo Linux Secu Advisory, GLSA 200 February 14, 2005**

Multiple Vendors ISC BIND 9.3; MandrakeSoft Linux Mandrake 10.1 X86_64, 10.1	A remote Denial of Service vulnerability exists in the 'authvalidated()' function due to an error in the validator. Upgrade available at: http://www.isc.org/index.pl Mandrake: http://www.mandrakesecure.net/en/ftp.php **Trustix:** **http://www.trustix.org/errata/2005/0003/** Currently we are not aware of any exploits for this vulnerability.	BIND Validator Self Checking Remote Denial of Service CVE Name: CAN-2005-0034	Low	US-CERT Vulnerabil VU#938617, January **Trustix Secure Linu Advisory, TSLSA-20 February 11, 2005**
Multiple Vendors KDE 2.0, BETA, 2.0.1, 2.1-2.1.2, 2.2-2.2.2	A vulnerability exists in 'kdesktop/lockeng.cc' and 'kdesktop/lockdlg.cc' due to insufficient return value checking, which could let a malicious user bypass the screensaver lock mechanism. Debian: http://security.debian.org/pool/updates/main/k/kdebase/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-009.html** Currently we are not aware of any exploits for this vulnerability.	KDE Screensaver Lock Bypass CVE Name: CAN-2005-0078	Medium	Debian Security Advi 660-1, January 26, 2 **RedHat Security Ad RHSA-2005:009-19, 10, 2005**
Multiple Vendors MandrakeSoft Corporate Server 3.0, x86_64, Linux Mandrake 10.0, AMD64, 10.1, X86_64;Novell Evolution 2.0.2l Ubuntu Linux 4.1 ppc, ia64, ia32; Ximian Evolution 1.0.3-1.0.8, 1.1.1, 1.2-1.2.4, 1.3.2 (beta)	A buffer overflow vulnerability exists in the main() function of the 'camel-lock-helper.c' source file, which could let a remote malicious user execute arbitrary code. Update available at: http://cvs.gnome.org/viewcvs/evolution/camel/camel-lock-helper.c?rev=1.7&hideattic=0&view=log Gentoo: http://security.gentoo.org/glsa/glsa-200501-35.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ SUSE: ftp://ftp.suse.com/pub/suse/ **Debian:** **http://security.debian.org/pool/updates/main/e/evolution/** Currently we are not aware of any exploits for this vulnerability.	Evolution Camel-Lock-Helper Application Remote Buffer Overflow CVE Name: CAN-2005-0102	High	Gentoo Linux Securit GLSA 200501-35, Ja 2005 Ubuntu Security Noti USN-69-1, January 2 Mandrakelinux Secur Advisory, MDKSA-20 January 27, 2005 SUSE Security Sumr Report, SUSE-SR:20 February 4, 2005 **Debian Security Adv DSA 673-1, Februar**
Multiple Vendors Perl	A race condition vulnerability was reported in the 'File::Path::rmtree()' function. A remote user may be able to obtain potentially sensitive information. A remote user may be able to obtain potentially sensitive information or modify files. The vendor has released Perl version 5.8.4-5 to address this vulnerability. Customers are advised to contact the vendor for information regarding update availability. Debian: http://security.debian.org/pool/updates/main/p/perl/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/perl/ OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/perl-5.8.4-2.1.1.src.rpm Gentoo:	Multiple Vendors Perl File::Path::rmtree() Permission Modification Vulnerability CVE Name: CAN-2004-0452	Medium	Ubuntu Security Noti USN-44-1, Decembe Debian Security Advi 620-1, December 30 OpenPKG Security A OpenPKG-SA-2005.0 January 11, 2005 Gentoo Linux Securit GLSA 200501-38, Ja 2005 **MandrakeSoft Secu Advisory, MDKSA-2 February 8, 2005** **SUSE Security Sum Report, SUSE-SR:2**

	http://security.gentoo.org/glsa/glsa-200501-38.xml **Mandrake:** **http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:031** **SUSE:** **ftp://ftp.suse.com/pub/suse/**			**February 11, 2005**
Multiple Vendors Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 .STABLE4&5, 2.4 .STABLE6&7, 2.4 .STABLE2, 2.4, 2.5 .STABLE3-7, 2.5 .STABLE1; Conectiva Linux 9.0, 10.0	Two vulnerabilities exist: remote Denial of Service vulnerability exists in the Web Cache Communication Protocol (WCCP) functionality due to a failure to handle unexpected network data; and buffer overflow vulnerability exists in the 'gopherToHTML()' function due to insufficient validation of user-supplied strings, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-wccp_denial_of_service.patch http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-gopher_html_parsing.patch Gentoo: http://security.gentoo.org/glsa/glsa-200501-25.xml Debian: http://security.debian.org/pool/updates/main/s/squid/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-061.html** **SUSE:** **ftp://ftp.suse.com/pub/suse/** **Trustix:** **http://www.trustix.org/errata/2005/0003/** There is no exploit required.	Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow CVE Names: CAN-2005-0094 CAN-2005-0095	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA January 13, 2005 Debian Security Advi 651-1, January 20, 2 Ubuntu Security Noti USN-67-1, January 2 Mandrakelinux Secur Advisory, MDKSA-20 January 25, 2005 Conectiva Linux Secu Announcement, CLA January 26, 2005 Fedora Update Notifi FEDORA-2005-105 & February 1, 2005 SUSE Security Sumr Report, SUSE-SR:20 February 4, 2005 **Trustix Secure Linu** **Advisory, TSLSA-20** **February 11, 2005** **SUSE Security Announcement, SUSE-SA:2005:006, 10, 2005** **RedHat Security Ad** **RHSA-2005:061-19, 11, 2005**

Multiple Vendors SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, x86_64, 9.1, 9.2; Squid Web Proxy Cache 2.5 .STABLE3-STABLE7, 2.5 .STABLE1	A vulnerability exists due to a failure to handle malformed HTTP headers. The impact was not specified. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-oversize_reply_headers.patch Gentoo: http://security.gentoo.org/glsa/glsa-200502-04.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-061.** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/s/squid/** Currently we are not aware of any exploits for this vulnerability.	Squid Proxy Malformed HTTP Headers CVE Name: CAN-2005-0174	Not Specified	Gentoo Linux Securit GLSA 200502-04:02, 2, 2005 SUSE Security Summ Report, SUSE-SR:20 February 4, 2005 US-CERT Vulnerabil VU#768702 US-CERT Vulnerabil VU#823350 **Ubuntu Security No USN-77-1 , February** **SUSE Security Announcement, SUSE-SA:2005:006, 10, 2005** **Mandrakelinux Secu Update Advisory, MDKSA-2005:034, F 11, 2005** **RedHat Security Ad RHSA-2005:061-19, 11, 2005**

Multiple Vendors
Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;
Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.20;
Gentoo Linux;
GNOME GPdf 0.112;
KDE KDE 3.2-3.2.3, 3.3, 3.3.1, kpdf 3.2;
RedHat Fedora Core2;
Ubuntu ubuntu 4.1, ppc, ia64, ia32, Xpdf Xpdf 0.90-0.93; 1.0.1, 1.0 0a, 1.0, 2.0 3, 2.0 1, 2.0, 3.0, SUSE Linux - all versions
	Several integer overflow vulnerabilities exist in 'pdftops/Catalog.cc' and 'pdftops/XRef.cc,' which could let a remote malicious user execute arbitrary code.
	Debian:
	http://security.debian.org/pool/updates/main/c/cupsys/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200410-20.xml
	KDE:
	ftp://ftp.kde.org/pub/kde/security_patches/post-3.3.1-kdegraphics.diff
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/
	Debian:
	http://security.debian.org/pool/updates/main/t/tetex-bin/
	SUSE: Update:
	ftp://ftp.SUSE.com/pub/SUSE
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200501-31.xml
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
		Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows
		CVE Names:
		CAN-2004-0888
		CAN-2004-0889
			High	SecurityTracker Alert 1011865, October 21
				Conectiva Linux Secu Announcement, CLA November 8, 2004
				Debian Security Advi 599-1, November 25,
				SUSE Security Summ Report, SUSE-SR:20 November 30, 2004
				Gentoo Linux Securit GLSA 200501-31, Ja 2005
				Fedora Update Noti FEDORA-2005-122, 133-136, February 8
				Fedora Legacy Upd Advisory, FLSA:235 February 10, 2005

	FedoraLegacy: **http://download.fedoralegacy.org/fedora/1/updates/** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Gentoo Linux, 1.4; Rob Flynn Gaim 0.10 x, 0.10.3, 0.50-0.75, 0.78, 0.82, 0.82.1, 1.0, 1.0.1; Slackware Linux -current, 9.0, 9.1, 10.0	A buffer overflow vulnerability exists in the processing of MSNSLP messages due to insufficient verification, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200410-23.xml Rob Flynn: http://prdownloads.sourceforge.net/gaim/gaim-1.0.2.tar.gz?download RedHat: ftp://updates.redhat.com Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.0/patches/packages/gaim-1.0.2-i486-1.tgz Ubuntu:http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Mandrake: http://www.mandrakesoft.com/security/advisories **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** We are not aware of any exploits for this vulnerability.	Gaim MSNSLP Remote Buffer Overflow CVE Name: CAN-2004-0891	High	Gentoo Linux Securit GLSA 200410-23, Oc 2004 RedHat Security Adv RHSA-2004:604-01, 20, 2004 Slackware Security A SSA:2004-296-01, O 2004 Ubuntu Security Noti USN-8-1 October 27, Mandrakelinux Secur Advisory, MDKSA-20 November 1, 2004 **Fedora Legacy Upd Advisory, FLSA:218 February 11, 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/pool/main/m/mailman/ There is no exploit code required.	GNU Mailman Remote Directory Traversal CVE Name: CAN-2005-0202	Medium	Debian Security Advi 674-1, February 10, 2 Ubuntu Security Noti USN-78-1, February Fedora Update Notifi FEDORA-2005-131 & February 10, 2005 Gentoo Linux Securit GLSA 200502-11, Fe 2005 RedHat Security Adv RHSA-2005:136-08, 10, 2005 Fedora Update Notifi FEDORA-2005-131 & February 10, 2005 Gentoo Linux Securit GLSA 200502-11, Fe 2005 Debian Security Advi DSA 674-1 & 674-2, 10 & 11, 2005 SUSE Security Anno SUSE-SA:2005:007, 14, 2005 Mandrakelinux Secur Advisory, MDKSA-20 February 14, 2005

Multiple Vendors
 	
Gentoo Linux;
RedHat Fedora Core3, Core2;
SUSE Linux 8.1, 8.2, 9.0-9.2, Desktop 1.0, Enterprise Server 9, 8, Novell Linux Desktop 1.0;
X.org X11R6 6.7 .0, 6.8, 6.8.1;
XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0-4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1
4.3 .0
	Multiple vulnerabilities exist due to integer overflows, memory access errors, input validation errors, and logic errors, which could let a remote malicious user execute arbitrary code, obtain sensitive information or cause a Denial of Service.
	
	Fedora:
	http://download.fedora.redhat.com /pub/fedora/linux/core/updates
	
	Gentoo:
	http://security.gentoo.org/ glsa/glsa-200411-28.xml
	
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	
	X.org:
	http://www.x.org/pub/
	
	Fedora:
	http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/2/
	
	RedHat:
	http://rhn.redhat.com/errata/ RHSA-2004-537.html
	
	Mandrakesoft:
	http://www.mandrakesoft.com/security/ advisories? name=MDKSA-2004:137 (libxpm)
	
	http://www.mandrakesoft.com/security/ advisories? name=MDKSA-2004:138 (XFree86)
	
	Debian:
	http://www.debian.org/ security/2004/dsa-607 (XFree86)
	
	SGI:
	ftp://patches.sgi.com/support/ free/security/patches/ProPack/3/
	
	TurboLinux:
	http://www.turbolinux.com/update/
	
	Avaya:
	http://support.avaya.com/elmodocs2/ security/ASA-2005-023_RHSA-2004-537.pdf
	
	http://support.avaya.com/elmodocs2/ security/ASA-2005-025_RHSA-2005-004.pdf
	
	Gentoo:
	http://security.gentoo.org/ glsa/glsa-200502-06.xml
	
	http://security.gentoo.org/ glsa/glsa-200502-07.xml
	
	Currently we are not aware of any exploits for these vulnerabilities.
		Multiple Vendors LibXPM Multiple Vulnerabilities
		
		CVE Name:
		CAN-2004-0914
			Low/
			Medium/
			High
			
			(Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)
				X.Org Foundation Se Advisory, November
				
				Fedora Update Notifi FEDORA-2004-433 & November 17 & 18, 2
				
				SUSE Security Anno SUSE-SA:2004:041, 17, 2004
				
				Gentoo Linux Securit GLSA 200411-28, No 19, 2004
				
				Fedora Security Upd Notifications FEDORA-2003-464, & 467, December 1,
				
				RedHat Security Adv RHSA-2004:537-17, 2, 2004
				
				Mandrakesoft:
				MDKSA-2004:137: lil MDKSA-2004:138: X November 22, 2004
				
				Debian Security Advi DSA-607-1 xfree86 - vulnerabilities, Decer 2004
				
				Turbolinux Security Announcement, Janu 2005
				
				Avaya Security Advis ASA-2005-023 & 025 25, 2005
				
				Gentoo Linux Secu Advisories, GLSA 2 & 07, February 7, 20

Multiple Vendors Larry Wall Perl 5.8, 5.8.1, 5.8.3, 5.8.4, 5.8.4 -1-5.8.4-5; Ubuntu Linux 4.1 ppc, ia64, ia32	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PERLIO_DEBUG' SuidPerl environment variable, which could let a malicious user execute arbitrary code; and a vulnerability exists due to an error when handling debug message output, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/universe/p/perl/ **Gentoo:** **http://security.gentoo.org/ glsa/glsa-200502-13.xml** **Mandrake:** **http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2005:031** **RedHat:** **http://rhn.redhat.com/errata/ RHSA-2005-105.html** **SGI:** **ftp://oss.sgi.com/projects/ sgi_propack/download/3/updates/** **SUSE:** **ftp://ftp.suse.com/pub/suse/** **Trustix:** **http://www.trustix.org/errata/2005/0003/** **Proofs of Concept exploits have been published.**	Perl SuidPerl Multiple Vulnerabilities CVE Names: CAN-2005-0155 CAN-2005-0156	Medium/ High (High if arbitrary code can be executed)	Ubuntu Security Noti USN-72-1, February **MandrakeSoft Secu Advisory, MDKSA-2 February 9, 2005** **RedHat Security Ad RHSA-2005:105-11, 7, 2005** **SGI Security Adviso 20050202-01-U, Feb 2005** **SUSE Security Sum Report, SUSE-SR:2(February 11, 2005** **Gentoo Linux Secur Advisory, GLSA 200 February 11, 2005** **Trustix Secure Linu Advisory, TSLSA-20 February 11, 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 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/** Another exploit script has been published.	Linux Kernel uselib() Root Privileges CVE Name: CAN-2004-1235	High	iSEC Security Resea Advisory, January 7, Fedora Update Notifi FEDORA-2005-013 & January 10, 2005 Trustix Secure Linux Advisory, TSLSA-200 January 13, 2005 Mandrake Security A MDKSA-2005:022, Ja 2005 PacketStorm, Januar **Avaya Security Adv ASA-2005-034, Febr 2005** **Ubuntu Security No USN-57-1, February**
Multiple Vendors Linux kernel 2.4.0-test1-test12, 2.4-2.4.28, 2.4.29 -rc1&rc2;**Avaya S8710/S8700/**	A vulnerability exists in the processing of ELF binaries on IA64 systems due to improper checking of overlapping virtual memory address allocations, which could let a malicious user cause a Denial of Service or potentially obtain root privileges. Patch available at: http://linux.bkbits.net:8080/linux-2.6/cset@	Linux Kernel Overlapping VMAs CVE Name: CAN-2005-0003	Low/High (High if root access can be	Trustix Secure Linux Advisory, TSLSA-200 January 13, 2005 RedHat Security Adv RHSA-2005:043-13 & RHSA-2005:017-14m

S8500/S8300, Converged Communication Server, Intuity LX, MN100, Modular Messaging, Network Routing	41a6721cce-LoPqkzKXudYby_3TUmg Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-043.html http://rhn.redhat.com/errata/RHSA-2005-017.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-034_RHSA-2005-016RHSA-2006-017RHSA-2005-043.pdf** Currently we are not aware of any exploits for this vulnerability.		obtained)	18 & 21, 2005 Mandrake Security A MDKSA-2005:022, Ja 2005 **Avaya Security Adv ASA-2005-034, Febr 2005**
Multiple Vendors Linux kernel 2.4-2.4.28; **Avaya S8710/S8700/ S8500/S8300, Converged Communication Server, Intuity LX, MN100, Modular Messaging, Network Routing**	A vulnerability exists in the device drivers due to failure to implement all required virtual memory access flags. RedHat: http://rhn.redhat.com/errata/RHSA-2005-016.html http://rhn.redhat.com/errata/RHSA-2005-017.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-034_RHSA-2005-016RHSA-2006-017RHSA-2005-043.pdf** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Device Driver Virtual Memory Flags Implementation Failure CVE Name: CAN-2004-1057	Not Specified	RedHat Security Adv RHSA-2005:016-13 & January 21, 2005 **Avaya Security Adv ASA-2005-034, Febr 2005**
Multiple Vendors Linux kernel 2.6 .10, 2.6-2.6.11	Multiple vulnerabilities exist: a vulnerability exists in the 'radeon' driver due to a race condition, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the 'i2c-viapro' driver, which could let a malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'locks_read_proc()' function, which could let a malicious user execute arbitrary code; a vulnerability exists in 'drivers/char/n_tty.c' due to a signedness error, which could let a malicious user obtain sensitive information; and potential errors exist in the 'atm_get_addr()' function and the 'reiserfs_copy_from_user_to_file_region()' function. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.11-rc4.bz2 Exploit scripts have been published.	Linux Kernel Multiple Local Buffer Overflows & Information Disclosure	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA February 15, 2005

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 Sun: http://sunsolve.sun.com/search/document.do ?assetkey=1-26-57646-1&searchclause= Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora Legacy: http://download.fedoralegacy.org/fedora/1/updates/ **SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.12** 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, SA September 16, 2004 Fedora Update Notifi FEDORA-2004-303, 21, 2004 Gentoo Linux Securit GLSA 200409-24, Se 17, 2004 Sun(sm) Alert Notifica 57646, October 7, 20 Conectiva Linux Secu Announcement, CLA October 26, 2004 Fedora Legacy Upda Advisory, FLSA:2076 November 5, 2004 **SCO Security Advis SCOSA-2005.12, Fe 2005**
Multiple Vendors Squid 2.x; Gentoo Linux;Ubuntu Linux 4.1 ppc, ia64, ia32;Ubuntu Linux 4.1 ppc, ia64, ia32; Conectiva Linux 9.0, 10.0	A remote Denial of Service vulnerability exists in the NTLM fakeauth_auth helper when running under a high load or for a long period of time, and a specially crafted NTLM type 3 message is submitted. Patch available at: http://www.squid-cache.org/Versions/v2/ 2.5/bugs/squid-2.5. STABLE7-fakeauth_auth.patch Gentoo: http://security.gentoo.org/glsa/ glsa-200501-25.xml Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates **RedHat: http://rhn.redhat.com/errata/ RHSA-2005-061.html** **SUSE: ftp://ftp.suse.com/pub/suse/** **Trustix: http://www.trustix.org/errata/2005/0003/** Currently we are not aware of any exploits for this vulnerability.	Squid NTLM fakeauth_auth Helper Remote Denial of Service CVE Name: CAN-2005-0096	Low	Secunia Advisory, SA13789, January 1 Gentoo Linux Securit GLSA 200501-25, Ja 2005 Ubuntu Security Noti USN-67-1, January 2 Conectiva Linux Secu Announcement, CLA January 26, 2005 Fedora Update Notifi FEDORA-2005-105 & February 1, 2005 SUSE Security Summ Report, SUSE-SR:20 February 4, 2005 **SUSE Security Announcement, SUSE-SA:2005:006, 10, 2005** **Trustix Secure Linu Advisory, TSLSA-20 February 11, 2005** **RedHat Security Ad RHSA-2005:061-19, 11, 2005**
MySQL MySQL 4.x	A vulnerability exists in the 'mysqlaccess.sh' script because temporary files are created in an unsafe manner, which could let a malicious user obtain elevated privileges. Update available at: http://lists.mysql.com/internals/20600	MySQL 'mysqlaccess.sh' Unsafe Temporary Files CVE Name: CAN-2005-0004	Medium	SecurityTracker Alert January 17,2005 Ubuntu Security Noti USN-63-1 January 1 Debian Security Advi

	Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-63-1 Debian: http://www.debian.org/security/2005/dsa-647 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-33.xml **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.			DSA-647-1 mysql, Ja 2005 Gentoo GLSA 20050 January 23, 2005 **Mandrakelinux Secu Update Advisory, MDKSA-2005:036, F 11, 2005** Trustix Secure Linux Advisory, TSLSA-200 February 11, 2005
Netkit Linux Netkit 0.17	A Denial of Service vulnerability exists when processing malformed size packets. Debian: http://security.debian.org/pool/updates/main/n/netkit-rwho/ Currently we are not aware of any exploits for this vulnerability.	Netkit RWho Malformed Packet Size Denial of Service CVE Name: CAN-2004-1180	Low	Debian Security Advi 678-1, February 11, 2

Open Group Open Motif 2.x, Motif 1.x; **Avaya CMS Server 8.0, 9.0, 11.0, CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing**	Multiple vulnerabilities have been reported in Motif and Open Motif, which potentially can be exploited by malicious people to compromise a vulnerable system. Updated versions of Open Motif and a patch are available. A commercial update will also be available for Motif 1.2.6 for users, who have a commercial version of Motif. http://www.ics.com/developers/index.php?cont=xpm_security_alert Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-537.html Gentoo: http://security.gentoo.org/glsa/glsa-200410-09.xml Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/x/xfree86/ TurboLinux: http://www.turbolinux.com/update/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-023_RHSA-2004-537.pdf http://support.avaya.com/elmodocs2/security/ASA-2005-025_RHSA-2005-004.pdf **Gentoo:** **http://security.gentoo.org/glsa/glsa-200502-07.xml** **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000924** Currently we are not aware of any exploits for these vulnerabilities.	Open Group Motif / Open Motif libXpm Vulnerabilities CVE Names: CAN-2004-0687 CAN-2004-0688	High	Integrated Computer Secunia Advisory ID: December 2, 2004 RedHat Security Adv RHSA-2004:537-17, 2, 2004 Turbolinux Security Announcement, Janu 2005 Avaya Security Advis ASA-2005-023 & 025 25, 2005 **SUSE Security Sum Report, SUSE-SR:20** **February 4, 2005** **Gentoo Linux Secur Advisory, GLSA 200** **February 7, 2005** **Conectiva Security CLSA-2005:924, Feb** **2005**
Open Webmail Open Webmail 1.7, 1.8, 1.71, 1.81, 1.90, 2.5, 2.20, 2.21, 2.30-2.32	A Cross-Site Scripting vulnerability exists in the 'logindomain' parameter due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://turtle.ee.ncku.edu.tw/openwebmail/download/cert/patches/SA-05:01/2.5x.patch There is no exploit code required.	Open WebMail 'Logindomain' Parameter Cross-Site Scripting CVE Name: CAN-2005-0445	High	Secunia Advisory, SA14253, February 1
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/**	Opera Default 'kfmclient exec' Configuration	High	Zone-H Advisory, ZH2004-19SA, Dece 2004 **Gentoo Linux Secur Advisory, GLSA 200** **February 14, 2005**

	glsa/glsa-200502-17.xml A Proof of Concept exploit has been published.			
PHP Group Debian Slackware Fedora pp 4.3.7 and prior	Updates to fix multiple vulnerabilities with php4 which could allow remote code execution. Debian: Update to Debian GNU/Linux 3.0 alias woody at http://www.debian.org/releases/stable/ Slackware: http://www.slackware.com/security/viewer.php?l=slackware- security&y=2004&m=slackware-security.406480 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/ Apple: http://www.apple.com/support/downloads/ **Debian:** **http://security.debian.org/pool/updates/main/p/php3/** An exploit script has been published.	PHP 'memory_limit' and strip_tags() Remote Vulnerabilities CVE Names: CAN-2004-0594 CAN-2004-0595	High	Secunia, SA12113 ar SA12116, July 21, 20 Debian, Slackware, a Security Advisories Turbolinux Security A TLSA-2004-23, Septe 2004 PacketStorm, Decem 2004 Apple Security Updat APPLE-SA-2005-01- January 26, 2005 **Debian Security Ad DSA, 669-1, Februar**

PNG Development Group Conectiva Debian Fedora Gentoo Mandrakesoft RedHat SUSE Sun Solaris HP-UX GraphicsMagick ImageMagick Slackware libpng 1.2.5 and 1.0.15	Multiple vulnerabilities exist in the libpng library which could allow a remote malicious user to crash or execute arbitrary code on an affected system. These vulnerabilities include: • libpng fails to properly check length of transparency chunk (tRNS) data, • libpng png_handle_iCCP() NULL pointer dereference, • libpng integer overflow in image height processing, • libpng png_handle_sPLT() integer overflow, • libpng png_handle_sBIT() performs insufficient bounds checking, • libpng contains integer overflows in progressive display image reading. If using original, update to libpng version 1.2.6rc1 (release candidate 1) available at: http://www.libpng.org/pub/png/libpng.html Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000856 Debian: http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00139.html Gentoo: http://security.gentoo.org/glsa/glsa-200408-03.xml Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:079 RedHat http://rhn.redhat.com/ SUSE: http://www.SUSE.de/de/security/2004_23_libpng.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Sun Solaris: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57617 HP-UX: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01065 GraphicsMagick: http://www.graphicsmagick.org/www/download.html ImageMagick: http://www.imagemagick.org/www/download.html Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.439243 Yahoo: http://messenger.yahoo.com/ SUSE: ftp://ftp.SUSE.com/pub/SUSE SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.16	Multiple Vulnerabilities in libpng CVE Names: CAN-2004-0597 CAN-2004-0598 CAN-2004-0599	High	US-CERT Technical Security Alert TA04-2 August 4, 2004 US-CERT Vulnerabil VU#160448, VU#388 VU#817368, VU#236 VU#477512, VU#286 August 4, 2004 SUSE Security Anno SUSE-SA:2004:035, 2004 SCO Security Adviso SCOSA-2004.16, Oc 2004 Fedora Legacy Upda Advisory, FLSA:2089 27, 2004 Sun(sm) Alert Notifica 57683, November 30 **Fedora Legacy Upd Advisory, FLSA:194 February 8, 2005**

	Fedora Legacy: http://download.fedoralegacy.org/redhat/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57683-1 **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit has been published.			
PowerDNS PowerDNS 2.0 RC1, 2.8, 2.9.15	A remote Denial of Service vulnerability exists in the'DNSPacket::expand' method in 'dnspacket.cc' due to a failure to handle exceptional conditions. Upgrades available at: http://www.powerdns.com/downloads/index.php Gentoo: http://security.gentoo.org/glsa/glsa-200502-15.xml Currently we are not aware of any exploits for this vulnerability.	PowerDNS Remote Denial of Service CVE Name: CAN-2005-0428	Low	Gentoo Linux Securit GLSA 200502-15, Fe 2005
SCO Open Server 5.0.6 a, 5.0.6, 5.0.7	Multiple buffer overflow vulnerabilities exist due to insecure copying of user-supplied input, which could let a malicious user execute arbitrary code. OpenServer 5.0.6: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.13/VOL.000.000 OpenServer 5.0.7: ftp://ftp.sco.com/pub/openserver5/507/mp/mp3/507mp3_vol.tar Currently we are not aware of any exploits for these vulnerabilities.	SCO OpenServer Multiple Local Buffer Overflows CVE Name: CAN-2004-1131	High	SCO Security Adviso SCOSA-2005.13, Fe 2005
Squid-cache.org Squid Web Proxy Cache 2.5 .STABLE5-STABLE8	A remote Denial of Service vulnerability exists when performing a Fully Qualify Domain Name (FQDN) lookup and and unexpected response is received. Patches available at: http://downloads.securityfocus.com/vulnerabilities/patches/ Currently we are not aware of any exploits for this vulnerability.	Squid Proxy FQDN Remote Denial of Service CVE Name: CAN-2005-0446	Low	Secunia Advisory, SA14271, February 1
SquirrelMail Development Team SquirrelMail 1.2.6	A vulnerability exists in 'src/webmail.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/squirrelmail_1.2.6-2_all.deb Currently we are not aware of any exploits for this vulnerability.	SquirrelMail Remote Code Execution CVE Name: CAN-2005-0152	High	Debian Security Advi 662-1, February 1, 20 **US-CERT Vulnerabi VU#203214**
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 There is no exploit code required.	SquirrelMail S/MIME Plug-in Remote Command Execution CVE Name: CAN-2005-0239	High	iDEFENSE Security February 7, 2005 US-CERT Vulnerabil VU#502328
Sun Microsystems, Inc. Sun Java JDK 1.5.x Sun Java JRE 1.1.x, 1.2.x, 1.3.x, 1.4.x, 1.5.x, SDK 1.1.x, 1.2.x, 1.3.x, SDK 1.4.x	A vulnerability exists in the in Sun Java Plugin due to the creation of temporary files that use a predictable filename, which could let a malicious user write arbitrary content to a file with a predictable name. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Sun Java Plugin Temporary File Predictable Filenames	Medium	US-CERT Vulnerabil VU#544392

Sun Microsystems, Inc. Solaris 8.0 _x86, 8.0, 9.0 _x86, 9.0; **Avaya CMS Server 9.0, 11.0, 12.0**	A Denial of Service vulnerability exists due to a failure to handle excessive UDP endpoint activity. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1-21-117351-16-1 **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-033_SUN-1-29-2005.pdf** Currently we are not aware of any exploits for this vulnerability.	Sun Solaris UDP Processing Denial of Service CVE Name: CAN-2005-0426	Low	Sun(sm) Alert Notific 57728, January 26, 2 **Avaya Security Adv ASA-2005-033, Febr 2005**
Sun Microsystems, Inc. Solaris 7.0, 7.0 _x86, 8.0, 8.0 _x86, 9.0, 9.0 _x86	A remote Denial of Service vulnerability exists due to a failure to handle a flood of ARP packets. Patches available at: http://classic.sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57673&zone_32=category%3Asecurity Currently we are not aware of any exploits for this vulnerability.	Sun Solaris ARP Handling Remote Denial of Service CVE Name: CAN-2005-0447	Low	Sun(sm) Alert Notific 57673, February 11,
Sympa Sympa 3.3.3	A buffer overflow vulnerability exists in 'src/queue.c' in the 'listname' parameter, which could let a malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/s/sympa/ Currently we are not aware of any exploits for this vulnerability.	Sympa 'src/queue.c' Buffer Overflow CVE Name: CAN-2005-0073	High	Debian Security Advi 677-1 , February 11,
Synaesthesia Synaesthesia 2.1 .0	A vulnerability exists due to a failure to secure access files, which could let a malicious user obtain sensitive information. Debian: http://security.debian.org/pool/updates/main/s/synaesthesia/ There is no exploit code required.	Synaesthesia Information Disclosure CVE Name: CAN-2005-0070	Medium	Debian Security Advi 681-1 , February 14,
xpcd xpcd 2.0 8	A buffer overflow vulnerability exists in 'pcdsvgaview' due to a failure to copy user-supplied input securely, which could let a malicious user execute arbitrary code. Update available at: http://security.debian.org/pool/updates/main/x/xpcd/ Currently we are not aware of any exploits for this vulnerability.	XPCD 'PCDSVGAView' Buffer Overflow CVE Name: CAN-2005-0074	High	Debian Security Advi 676-1 , February 11,
xview xview 3.2 p1.4	Multiple buffer overflow vulnerabilities exist in the xview library, which could let a malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/x/xview/ Currently we are not aware of any exploits for these vulnerabilities.	XView Multiple Buffer Overflows CVE Name: CAN-2005-0076	High	Debian Security Advi 672-1, February 9, 20
Yongguang Zhang hztty 2.0	A vulnerability exists due to an unknown cause, which could let a malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/h/hztty/ Currently we are not aware of any exploits for this vulnerability.	Yongguang Zhang HZTTY Arbitrary Command Execution CVE Name: CAN-2005-0019	High	Debian Security Advi 675-1, February 10, 2
Yukihiro Matsumoto Ruby 1.8.x	A remote Denial of Service vulnerability exists due to an input validation error in 'cgi.rb.' Debian: http://security.debian.org/pool/updates/main/r/ruby Mandrake: http://www.mandrakesoft.com/security/advisories	Yukihiro Matsumoto Ruby Infinite Loop Remote Denial of Service CVE Name: CAN-2004-0983	Low	Secunia Advisory, SA13123, November Ubuntu Security Noti USN-20-1, Novembe Fedora Update Notifi FEDORA-2004-402 & November 11 & 12, 2 Gentoo Linux Securit

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/r/ruby1.8/l Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-23.xml Red Hat: http://rhn.redhat.com/errata/RHSA-2004-635.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-635.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.			GLSA 200411-23, No 16, 2004 Red Hat Advisory, RHSA-2004:635-03, 13, 2004 RedHat Security Adv RHSA-2004:635-06, 17, 2005 SGI Security Advisor 20050101-01-U, Janu 2005 Turbolinux Security Announcement, 2005 January 31, 2005 **SUSE Security Sum Report, SUSE-SR:20 February 11, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apache mod_python	A vulnerability exists in mod_python in the publisher handler that could permit a remote malicious user to view certain python objects. A remote user can submit a specially crafted URL to view the names and values of variables. Red Hat: http://rhn.redhat.com/errata/RHSA-2005-104.html Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-80-1 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200502-14.xml Trustix: http://www.trustix.org/errata/2005/0003/ Currently we are not aware of any exploits for this vulnerability.	Apache mod_python Information Disclosure Vulnerability CVE Name: CAN-2005-0088	Medium	SecurityTracker Alert ID: 1013156, February 11, 2005 Red Hat RHSA-2005:104-03, February 10, 2005 Ubuntu, USN-80-1 February 11, 2005 Trustix #2005-0003, February 11, 2005
Barracuda Networks Barracuda Spam Firewall 3.1.10 and prior	A vulnerability exists that could permit white-listed senders to use the product as an open mail relay. Update to firmware 3.1.11 or later. Currently we are not aware of any exploits for this vulnerability.	Barracuda Spam Firewall 200 Open Mail Relay Vulnerability CVE Name: CAN-2005-0431	Low	Secunia SA14243, February 11, 2005

BEA Systems BEA WebLogic 8.1 through 8.1 SP3; 7.0 through 7.0 SP5	A vulnerability exists that could permit a remote malicious user to determine the reason for a failed authentication attempt. This allows a remote user to conduct a brute force password guessing attack. For WebLogic Server 8.1, upgrade to WebLogic Server 8.1 Service Pack 4. For WebLogic Server 7.0, upgrade to WebLogic Server 7.0 Service Pack 5 and then apply the following patch: ftp://ftpna.beasys.com/pub/releases/security/CR184612_70sp5.jar This fix will be included in WebLogic Server 7.0 Service Pack 6. Currently we are not aware of any exploits for this vulnerability.	BEA WebLogic Authentication Vulnerability CVE Name: CAN-2005-0432	Medium	BEA Security Advisory, BEA05-74.00
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.** Currently we are not aware of any exploits for this vulnerability.	Cisco IOS BGP Packets Denial of Service	Low	Cisco Security Advisory 63845, January 29, 2005 Technical Cyber Security Alert, TA05-026A, January 26, 2005 US-CERT Vulnerability Note VU#689326, January 26, 2005 **Cisco Security Advisory 63845, Revision 1.4, February 9, 2005**
Francisco Burzi PHP-Nuke 6.x-7.6	Multiple vulnerabilities exist that could permit a remote user to determine the installation path or conduct Cross-Site Scripting attacks. The Downloads module does not properly validate user-supplied input in the 'newdownloadshowdays' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Francisco Burzi PHP-Nuke Input Validation Vulnerability CVE Names: CAN-2005-0433 CAN-2005-0434	High	SecurityFocus, Bugtraq ID 12561, February 15, 2005
F-Secure F-Secure Anti-Virus for multiple platforms	A buffer overflow vulnerability exists when processing ARJ archives. A remote malicious user can execute arbitrary code on the target system because of input validation errors. This vulnerability can be exploited on some systems without user interaction. Vendor updates are available: http://www.f-secure.com/security/fsc-2005-1.shtml Currently we are not aware of any exploits for this vulnerability.	F-Secure Anti-Virus Buffer Overflow Vulnerability CVE Name: CAN-2005-0350	High	F-Secure Security Bulletin FSC-2005-1, February 10, 2005
F-Secure F-Secure Internet Gatekeeper version 6.41 and earlier; F-Secure Internet Gatekeeper for Linux 2.06	A buffer overflow vulnerability exists when processing ARJ archives. A remote malicious user can execute arbitrary code on the target system because of input validation errors. Vendor patches are available: http://www.f-secure.com/security/fsc-2005-1.shtml Currently we are not aware of any exploits for this vulnerability.	F-Secure Internet Gatekeeper Buffer Overflow Vulnerability CVE Name: CAN-2005-0350	High	F-Secure Security Bulletin FSC-2005-1, February 10, 2005
GNU Armagetron 0.2.6.0 and prior	Multiple vulnerabilities exist that could permit a remote malicious user to cause a Denial of Service in the target game service. This is due to buffer overflow and wait state errors. No workaround or patch available at time of publishing. An exploit script has been published.	GNU Armagetron Denial of Service Vulnerability CVE Name: CAN-2005-0369 CAN-2005-0370 CAN-2005-0371	Low	SecurityTracker Alert ID: 1013180, February 15, 2005
GNU AWStats 5.0-5.9, 6.0-6.2	Several vulnerabilities exist: a vulnerability exists in the 'awstats.pl' script due to insufficient validation of the 'configdir' parameter, which could let a remote malicious user execute arbitrary code; and an unspecified input validation vulnerability	GNU AWStats Multiple Remote Input Validation	High	Securiteam, January 18, 2005 **Gentoo Linux**

	exists. Upgrades available at: http://awstats.sourceforge.net/files/awstats-6.3.tgz SuSE: ftp://ftp.suse.com/pub/suse/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-36.xml** Currently we are not aware of any exploits for these vulnerabilities.	CVE Name: CAN-2005-0116		**Security Advisory [UPDATE] GLSA 200501-36:03, February 14, 2005** **US-CERT Vulnerability Note VU#272296**
GNU AWStats 6.3 and prior	Multiple vulnerabilities exist which could permit local malicious users to gain escalated privileges, disclose system information, and cause a Denial of Service. This is due to errors in "awstats.pl" and the "loadplugin" and "pluginmode" parameters input validation. The vulnerabilities have reportedly been fixed in the CVS repository. A Proof of Concept exploit has been published.	GNU AWStats Multiple Vulnerabilities CVE Names: CAN-2005-0435 CAN-2005-0436 CAN-2005-0437 CAN-2005-0438	Low/ Medium (Medium if sensitive information can be obtained or elevated privileges are obtained)	SecurityFocus, Bugtraq ID 12545, February 14, 2005
GNU CitrusDB prior to 0.3.6	A vulnerability exists that could permit a remote malicious user to obtain credit card import and export data. The vendor has issued a fixed version (0.3.6), available at: http://www.citrusdb.org/download.php **A Proof of Concept exploit has been published.**	GNU CitrusDB Data Disclosure CVE Name: **CAN-2005-0229**	Medium	OSVDB Reference: 13228, January 28, 2005 **SecurityFocus, 12402, February 13, 2005**
GNU ELOG 2.5.6 and prior	Two vulnerabilities exist that could permit disclosure of sensitive information or remote code execution. This is because of an input validation error and unprotected configuration file. Update to version 2.5.7: http://midas.psi.ch/elog/download.html A Proof of Concept exploit has been published.	GNU ELOG Disclosure and Code Execution Vulnerabilities CVE Names: CAN-2005-0439 CAN-2005-0440	High	SecurityFocus, Bugtraq ID 12556, February 15, 2005
GNU Siteman 1.1.0 - 1.1.10	A vulnerability exists that could permit a malicious user to bypass certain security restrictions. This is due to an unspecified error in "users.php." Apply patch: http://prdownloads.sourceforge.net/sitem/1.1.10x_patch.zip?download Currently we are not aware of any exploits for this vulnerability.	GNU Siteman Security Bypass Vulnerability CVE Name: CAN-2005-0305	Medium	Sourceforge.net, Siteman Release Notes 1.1.10x_patch
GPL Emdros 1.x	Multiple vulnerabilities due to memory leaks within the MQL parse which could permit a Denial of Service. Update to version 1.1.22: http://emdros.org/download.html Currently we are not aware of any exploits for these vulnerabilities.	GPL Emdros MQL Parser Denial of Service Vulnerability CVE Name: CAN-2005-0415	Low	SourceForge.net, Project Emdros, [1116935], February 8, 2005
GPL MercuryBoard 1.1.1	An input validation vulnerability in the 'func/post.php' script could permit a remote malicious user to inject SQL commands. The vendor has issued a fixed version (1.1.2), available at: http://www.mercuryboard.com/index.php?a=downloads A Proof of Concept exploit has been published.	GPL MercuryBoard SQL Injection Vulnerability CVE Name: CAN-2005-0414	High	SecurityTracker Alert ID: 1013137, February 9, 2005
GPL MyPHP Forum	A vulnerability exists that could permit a remote malicious user to inject SQL commands. This is because several scripts do not properly validate user-supplied input in certain fields. These scripts are: 'forum.php', 'member.php', 'forgot.php', and	GPL MyPHP Forum SQL Injection Vulnerability	High	SecurityTracker Alert ID: 1013136, February 9, 2005

	'include.php'. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	CVE Name: CAN-2005-0413		
Hewlett-Packard HP HTTP Server 5.0 through 5.95	A buffer overflow vulnerability exists that could permit a remote malicious user to execute arbitrary code on the target system or cause a Denial of Service. The vendor has issued a fixed version (5.96 or later). Alternately, the vendor indicates that you can update to the System Management Homepage Version 2.0 or later. Management Software Security Patch for Windows Version 5.96 (or later) is available at: http://h18023.www1.hp.com/support/files/Server/us/download/22192.html Currently we are not aware of any exploits for this vulnerability.	HP HTTP Server Buffer Overflow Vulnerability	Low/High (High if arbitrary code can be executed)	HP Security Bulletin, HPSBMA01116, February 14, 2005
IBM DB2 Universal Database 8.x	Multiple vulnerabilities exist that could permit a malicious user to cause a Denial of Service, obtain knowledge of sensitive information, read and manipulate file content, or execute arbitrary code. Apply DB2 8.1 FixPak 8: http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html Currently we are not aware of any exploits for these vulnerabilities.	IBM DB2 Universal Database Multiple Vulnerabilities CVE Name: CAN-2005-0417	Medium/ High (High if arbitrary code can be executed)	IBM Advisory, Reference #: 1196289, January 20, 2005
Jelsoft Enterprises VBulletin VBulletin 3.0 Gamma, beta 2-beta7. 3.0-3.0.4	A vulnerability exists in the 'forumdisplay.php' script due to insufficient sanitization when the 'showforumusers' option is enabled, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit required; however, a Proof of Concept exploit has been published.	Jelsoft VBulletin 'Forumdisplay.PHP' Script Remote Command Execution CVE Name: CAN-2005-0429	High	SecurityFocus, February 14, 2005
Mozilla Firefox 1.0	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 A Proof of Concept exploit has been published.	Mozilla Firefox Multiple Vulnerabilities CVE Name: CAN-2005-0230 CAN-2005-0231 CAN-2005-0232	High	SecurityTracker Alert ID: 1013108, February 8, 2005
Multiple Vendors Debian Linux 3.0 spar, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.7	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the DICOM dissector; a remote Denial of Service vulnerability exists in the handling of RTP timestamps; a remote Denial of Service vulnerability exists in the HTTP dissector; and a remote Denial of Service vulnerability exists in the SMB dissector when a malicious user submits specially crafted SMB packets. Potentially these vulnerabilities may also allow the execution of arbitrary code. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200412-15.xml Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-011.html SuSE:	Ethereal Multiple Denial of Service & Potential Code Execution Vulnerabilities CVE Names: CAN-2004-1139 CAN-2004-1140 CAN-2004-1141 CAN-2004-1142	Low/High (High if arbitrary code can be executed)	Ethereal Security Advisory, enpa-sa-00016, December 15, 2004 Conectiva Linux Security Announcement, CLA-2005:916, January 13, 2005 RedHat Security Advisory, RHSA-2005:011-11, February 2, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 **SGI Security Advisory, 20050202-01-U,**

	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 these vulnerabilities.			**February 9, 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. A Proof of Concept exploit has been published.	Multiple Vendors OpenPGP CFB Mode Vulnerable to Cipher-Text Attack CVE Name: CAN-2005-0366	Medium	US-CERT Vulnerability Note VU#303094
OpenConf OpenConf 1.0 4	An HTML injection vulnerability exists is due to input validation errors. This may permit a malicious user to execute arbitrary code. Disclosure of cookie-based credentials is also possible. Upgrade to OpenConf 1.10: http://www.zakongroup.com/technology/openconf-download.php There is no exploit required.	OpenConf Paper Submission HTML Injection Vulnerability CVE Name: CAN-2005-0407	High	SecurityFocus, Bugtraq ID 12554, February 15, 2005
Opera Software Opera	A spoofing vulnerability exists that could permit a malicious website to spoof the URL displayed in the address bar, SSL certificate, and status bar. This is due to an unintended result of the IDN (International Domain Name) implementation, which allows using international characters in domain names. **Gentoo: http://security.gentoo.org/glsa/glsa-200502-17.xml** A Proof of Concept exploit has been published.	Opera IDN Spoofing CVE Name: CAN-2005-0235	Medium	SecurityTracker Alert ID: 1013096, February 7, 2005 **Gentoo GLSA 200502-17, February 14, 2005**
Python SimpleXMLRPCServer 2.2 all versions, 2.3 prior to 2.3.5, 2.4	A vulnerability exists in the SimpleXMLRPCServer library module that could permit a remote malicious user to access internal module data, potentially executing arbitrary code. Python XML-RPC servers that use the register_instance() method to register an object without a _dispatch() method are affected. Patches for Python 2.2, 2.3, and 2.4, available at: http://python.org/security/ PSF-2005-001/patch-2.2.txt (Python 2.2) http://python.org/security/ PSF-2005-001/patch.txt (Python 2.3, 2.4) The vendor plans to issue fixed versions for 2.3.5, 2.4.1, 2.3.5, and 2.4.1. Debian: http://www.debian.org/security/ 2005/dsa-666 **Gentoo:** **http://security.gentoo.org/glsa/glsa-200502-09.xml** **Mandrakesoft:** **http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2005:035** **Trustix:** **http://www.trustix.org/errata/2005/0003/** **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2005-109.html** Currently we are not aware of any exploits for this vulnerability.	Python SimpleXMLRPCServer Remote Code CVE Name: CAN-2005-0089 **CAN-2005-0088**	High	Python Security Advisory: PSF-2005-001, February 3, 2005 **Gentoo, GLSA 200502-09, February 08, 2005** **Mandrakesoft, MDKSA-2005:035, February 10, 2005** **Trustix #2005-0003, February 11, 2005** **RedHat Security Advisory, RHSA-2005:109-04, February 14, 2005**

Spidean PostWrap	An input validation vulnerability exists that could permit a malicious remote user to conduct Cross-Site Scripting attacks. The module is designed to let remote web pages to be displayed on the target web site. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Spidean PostWrap Cross-Site Scripting Vulnerability CVE Name: CAN-2005-0412	High	Internet Security Systems, postwrap-xss (19261), February 9, 2005
Squid-cache.org Squid 2.5	A vulnerability exists that could permit a remote malicious user to send multiple Content-length headers with special HTTP requests to corrupt the cache on the Squid server. A patch (squid-2.5.STABLE7-header_parsing.patch) is available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-header_parsing.patch Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000923 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200502-04.xml Debian: http://www.debian.org/security/2005/dsa-667 Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-77-1 SuSE: ftp://ftp.suse.com/pub/suse/ **Trustix:** **http://www.trustix.org/errata/2005/0003/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-061.html** **SuSE:** **ftp://ftp.suse.com/pub/suse/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/s/squid/** Currently we are not aware of any exploits for this vulnerability.	Squid Error in Parsing HTTP Headers CVE Name: **CAN-2005-0174** CAN-2005-0175	Medium	SecurityTracker Alert ID, 1012992, January 25, 2005 Gentoo GLSA 200502-04, February 2, 2005 Debian DSA-667-1, February 4, 2005 SUSE, SUSE-SR:2005:003, February 4, 2005 US-CERT Vulnerability Note, VU#924198 US-CERT Vulnerability Note, VU#625878 **Trustix #2005-0003, February 11, 2005** **Ubuntu Security Notice, USN-77-1, February 7, 2005** **SUSE Security Announcement, SUSE-SA:2005:006, February 10, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:034, February 11, 2005** **RedHat Security Advisory, RHSA-2005:061-19, February 11, 2005**
SquirrelMail Development Team SquirrelMail 1.x	A Cross-Site Scripting vulnerability exists in the 'decodeHeader()' function in 'mime.php' when processing encoded text in headers due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://prdownloads.sourceforge.net/squirrelmail/sm143a-xss.diff?download Gentoo: http://security.gentoo.org/glsa/glsa-200411-25.xml Conectiva: ftp://atualizacoes.conectiva.com.br/9 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Apple:	SquirrelMail Cross-Site Scripting CVE Name: CAN-2004-1036 CAN-2005-0104 CAN-2005-0152	High	Secunia Advisory, SA13155, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-25, November 17, 2004 Fedora Update Notifications, FEDORA-2004-471 & 472, November 28, 2004 Conectiva Linux Security Announcement, CLA-2004:905, December 2, 2004

	http://www.apple.com/support/downloads/ SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://www.debian.org/security/2005/dsa-662 **Red Hat: http://rhn.redhat.com/errata/RHSA-2005-135.html** An exploit script is not required.			Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 Debian DSA-662-1, February 1, 2005 **Red Hat RHSA-2005:135-04, February 10, 2005**

Symantec
Norton AntiVirus for Microsoft Exchange 2.1, prior to build 2.18.85;
Symantec Norton Antivirus 2004 for Windows;
Symantec Norton Antivirus 2004 for Macintosh;
Symantec Norton Antivirus 9.0 for Macintosh
	A buffer overflow vulnerability exists that could permit a remote malicious user to execute arbitrary code on the target system. The DEC2EXE engine does not properly parse UPX compressed files when inspecting them for viruses.
	A fix is available via LiveUpdate and at:
	http://www.symantec.com/techsupp
	Currently we are not aware of any exploits for this vulnerability.
		Symantec Norton Anti-Virus Buffer Overflow
		CVE Name:
		CAN-2005-0249
			High	Symantec Security Response, SYM05-003, February 8, 2005
				US-CERT Vulnerability Note VU#107822

University of California (BSD License) PostgreSQL 7.x, 8.x	Multiple vulnerabilities exist that could permit malicious users to gain escalated privileges or execute arbitrary code. These vulnerabilities are due to an error in the 'LOAD' option, a missing permissions check, an error in 'contrib/intagg,' and a boundary error in the plpgsql cursor declaration. Update to version 8.0.1, 7.4.7, 7.3.9, or 7.2.7: http://wwwmaster.postgresql.org/download/mirrors-ftp Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-71-1 Debian: http://www.debian.org/security/2005/dsa-668 Gentoo: http://security.gentoo.org/glsa/glsa-200502-08.xml 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/p/postgresql/** **RedHat: http://rhn.redhat.com/errata/RHSA-2005-141.html** **Gentoo: http://security.gentoo.org/glsa/glsa-200502-19.xml** **Debian:** **http://security.debian.org/pool/updates/main/p/postgresql/** Currently we are not aware of any exploits for these vulnerabilities.	University of California PostgreSQL Multiple Vulnerabilities CVE Name: **CAN-2005-0227** **CAN-2005-0246** **CAN-2005-0244** **CAN-2005-0245** **CAN-2005-0247**	Medium/ High (High if arbitrary code can be executed)	PostgreSQL Security Release, February 1, 2005 Ubuntu Security Notice USN-71-1 February 01, 2005 Debian Security Advisory DSA-668-1, February 4, 2005 Gentoo GLSA 200502-08, February 7, 2005 Fedora Update Notifications, FEDORA-2005-124 & 125, February 7, 2005 **Ubuntu Security Notic,e USN-79-1 , February 10, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005** **Gentoo Linux Security Advisory, GLSA 200502-19, February 14, 2005** **RedHat Security Advisory, RHSA-2005:141-06, February 14, 2005** **Debian Security Advisory, DSA 683-1,**

[back to top]

Recent Exploit Scripts/Techniques

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

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

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
February 14, 2005	cabrightstor_disco.pm brightstor.c.php	Yes	Script that exploits the BrightStor ARCserve Backup Discovery Service Buffer Overflow vulnerability.
February 14, 2005	ex_perl.c ex_perl2.c	Yes	Proofs of Concept exploits for the Perl SuidPerl Multiple Vulnerabilities.
February 12, 2005	ecl-eximspa.c p_exim.c	Yes	Exploit for the GNU Exim Buffer Overflows vulnerability.
February 11, 2005	rkhunter-1.2.0.tar.gz	N/A	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
February 10, 2005	atronboom.zip	No	Exploit for the Armagetron Advanced Multiple Remote Denial of Service Vulnerabilities.
February 10, 2005	msnMessengerPNGexploit.c	Yes	Script that exploits the Windows/MSN Messenger PNG Processing vulnerability.
February 8, 2005	fm-afp.c	No	Script that exploits the Apple Mac OS X AppleFileServer Remote Denial of Service vulnerability.
February 8, 2005	rna_deleter.rgp rna_bof.rgs	No	Exploits for the RealNetworks RealArcade Multiple Remote Vulnerabilities.
February 7, 2005	3csploit.c	No	Script that exploits the 3Com 3CServer FTP Command Buffer Overflows vulnerability.
February 7, 2005	pde.txt	Yes	Exploit for the PerlDesk 'view' Parameter Input Validation vulnerability.
February 7, 2005	xfinder-ds.pl	No	Perl script that exploits the Apple Mac OS X Finder 'DS_Store' Insecure File Creation vulnerability.

[back to top]

Trends

- IBM has announced the results from its 2004 Global Business Security Index Report for potential security threats in 2005. For more information, see "IBM Security Report Predicts Mobile/Satellite Attacks in 2005," located at: http://sys-con.com/story/?storyid=48190&DE=1.
- An Internet browser feature that permits web addresses in Chinese, Arabic, and other languages could encourage online fraudsters by making scam Web sites look legitimate to visitors due to a lack of support internationalized domain names. For more information, see " Browser Feature Could Make Scams Easier," located at: http://www.washingtonpost.com/wp-dyn/articles/A5709-2005Feb7.html?sub=AR.
- WholeSecurity announced the industry's first worldwide anti-phishing network (www.phishreport.net). For more information, see "Microsoft, EBay, Paypal, And Visa Join WholeSecurity To Launch Phish Report Network, The Internet's First Global Anti-Phishing Aggregation Service" located at: http://www.phishreport.net/releases/launch_release.html and "Microsoft, eBay join antiphishing initiative" located at: http://news.com.com/Microsoft%2C+eBay+join+antiphishing+initiative/2100-1029_3-5575106.html.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

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

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-D	Win32 Worm	Stable	December 2004
3	Netsky-Q	Win32 Worm	Stable	March 2004
4	Zafi-B	Win32 Worm	Slight Increase	June 2004
5	Netsky-D	Win32 Worm	Slight Increase	March 2004
6	Sober-I	Win32 Worm	Decrease	November 2004
7	Bagle.bj	Win32 Worm	Stable	January 2005
8	Netsky-B	Win32 Worm	Stable	February 2004
9	Bagle.z	Win32 Worm	Stable	April 2004
10	Bagle-AU	Win32 Worm	Stable	October 2004

Table Updated February 15, 2005

Viruses or Trojans Considered to be a High Level of Threat

- Troj/BankAsh-A: Anti-virus firms said they uncovered the first malware, Troj/BankAsh-A, that switches off Microsoft AntiSpyware, along with its other functions. Troj/BankAsh-A includes a keylogger and attempts to steal credit card details, turn off other anti-virus applications, delete files, install other malicious code and download code from the Internet. For more information see: http://www.eweek.com/article2/0,1759,1763560,00.asp

- Worm_Aimdes.A: Last week saw instant messaging (IM) viruses and worms hit popular IM systems from both Microsoft and AOL. In the Microsoft MSN Messenger case, exploit code that could be used to create an IM virus was published on the Web. AOL's AIM was hit with a virus dubbed Worm_Aimdes.A. The virus sends a copy of itself to all online contacts in an affected user's Buddy List, sending a message in an attempt to trick recipient into thinking the file was send from a trusted source. For more information see: http://www.infoworld.com/article/05/02/11/HNimvirus_1.html

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

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

Name	Aliases	Type
Backdoor.Netshadow	Backdoor.Win32.NetShadow.a	Trojan
Downloader-ME.dr		Trojan
Mydoom.AK	W32/Mydoom.AK.worm	Win32 Worm
PWS-Banker.j	PWS-Banker.j.dll	Trojan
PWSteal.Bancos.O	PWS-Banker.f Trojan-Spy.Win32.Banker.jj TROJ_BANKER.EY Win32.Formglieder.D	Trojan
PWSteal.Bancos.P	PWS-Banker.f Trojan-Spy.Win32.Banker.jj TROJ_BANKER.EY	Trojan
PWSteal.Bankash.A	PWS-Banker.j PWSteal.Bankash.A Troj/BankAsh-A Trojan-Downloader.Win32.Small.ain	Trojan
Troj/LowZone-O	Trojan.Win32.LowZones.o	Trojan

TROJ_BANKER.EY		Trojan
TROJ_SPYBANK.A		Trojan
Trojan.Eneles		Trojan
Trojan.KillAV.E		Trojan
Trojan.Rplay.A		Trojan
VBS/Mcon-G	VBS.Mcon.c VBS/Pica.worm.gen VBS.Sorry.A VBS_MCON.A	Visual Basic Worm
W32.Kipis.J@mm		Win32 Worm
W32.Mydoom.AS@mm		Win32 Worm
W32.Randex.COX		Win32 Worm
W32/Agobot-PQ		Win32 Worm
W32/Agobot-PR		Win32 Worm
W32/Bropia.worm	WORM_BROPIA.I	Win32 Worm
W32/Bropia-J	Bropia.J W32/Bropia.J.worm	Win32 Worm
W32/Codbot-B		Win32 Worm
W32/Dopbot-A	Backdoor.Win32.IRCBot.q WORM_DOPBOT.A	Win32 Worm
W32/Mydoom.ba@MM	Email-Worm.Win32.Mydoom.ak W32.Mydoom.AU@mm W32/Mydoom.ba@MM	Win32 Worm
W32/MyDoom-AQ		Win32 Worm
W32/MyDoom-AR	W32/Mydoom.ba@MM	Win32 Worm
W32/MyDoom-AR	WORM_MYDOOM.AR	Win32 Worm
W32/Rbot-ALO	WORM_RBOT.ALO	Win32 Worm
W32/Rbot-TF		Win32 Worm
W32/Rbot-VQ		Win32 Worm
W32/Rbot-VT		Win32 Worm
W32/Rbot-VX		Win32 Worm
W32/Sdbot-UW		Win32 Worm
W32/Sdbot-UZ		Win32 Worm
W97M.Lebani		IRC Worm
W97M.MJ		IRC Worm
Win32.BettInet	Win32.BettInet.C Win32.BettInet.C!CAB Win32.BettInet.D Win32.BettInet.E Win32.BettInet.F Win32.BettInet.F!CAB	Win32 Worm
Win32.Faxbat	BackDoor-CMA Backdoor.Win32.Agent.ek W32.SillyP2P Win32.Faxbat.A Win32.Faxbat.B Win32/Faxbat.A!DLL!Worm Win32/Faxbat.B.Worm Win32/SillyP2P.L!P2P!Worm	Win32 Worm
Win32.Imiserv Family		Trojan
Win32.Linkbot Family		Win32 Worm
Win32.Mugly Family		Win32 Worm
Win32.Mydoom.AP	Email-Worm.Win32.Mydoom.ak W32/Mydoom.ba@MM Win32/Mydoom.33792!Worm	Win32 Worm
Win32.Mydoom.AQ	Email-Worm.Win32.Mydoom.ak W32/MyDoom-AR W32/Mydoom.ba@MM Win32/Mydoom.33792.A!Worm	Win32 Worm

	WORM_MYDOOM.AR	
Win32.Mydoom.AR	Email-Worm.Win32.Mydoom.ak W32/MyDoom-AR W32/Mydoom.ba@MM Win32/MyDoom.BA!Worm WORM_MYDOOM.AR	Win32 Worm
WORM_AHKER.C		Win32 Worm
WORM_AIMDES.A	IM-Worm.Win32.Aimes.a W32.Aimdes.A@mm W32/AimDes.worm	Win32 Worm
WORM_BROPIA.H		Win32 Worm
WORM_BROPIA.J		Win32 Worm
WORM_BROPIA.M	IM-Worm.Win32.VB.g W32.Bropia.M W32/Bropia-M W32/Bropia.worm.m	Win32 Worm
WORM_BROPIA.N		Win32 Worm
WORM_KIPIS.E		Win32 Worm
WORM_SDBOT.ANY		Win32 Worm

[back to top]

Last updated February 16, 2005