

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

Bugs, Holes, & Patches

- Windows Operating Systems
 - [Allied Telesyn AT-TFTP Server Arbitrary File Execution or Denial of Service](#)
 - [Apple QuickTime Integer Overflow](#)
 - [Akella Age of Sail II Buffer Overflow \(Updated\)](#)
 - [Code-Crafters Ability Server Buffer Overflow \(Updated\)](#)
 - [Global Spy Software Cyber Web Filter IP Address Restriction Security Bypass](#)
 - [Google Desktop Search 'meta' Tag Input Validation](#)
 - [Imspire GSuite Passwords Disclosure](#)
 - [Kingsoft XDICT Word Translation Buffer Overflow](#)
 - [MailEnable Professional Unspecified Webmail](#)
 - [Microsoft Internet Explorer/Outlook Express Restricted Zone Status Bar Spoofing](#)
 - [Microsoft Internet Explorer Font Tag Denial of Service](#)
 - [Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow](#)
 - [Microsoft Internet Explorer HHCtrl ActiveX Control Cross-Domain Scripting](#)
 - [Microsoft Remote Desktop on Windows XP Denial of Service](#)
 - [Microsoft NNTP Remote Code Execution \(Updated\)](#)
 - [Microsoft Windows Shell Remote Code Execution \(Updated\)](#)
 - [Multiple Vendor Anti-Virus Software Detection Evasion \(Updated\)](#)
 - [Tabs Laboratories MailCarrier EHLO SMTP Commands Buffer Overflow SMTP Commands](#)
 - [Website Pros NetObjects Fusion JPEG Processing Buffer Overflow](#)
- UNIX / Linux Operating Systems
 - [Apache mod_ssl Denial of Service \(Updated\)](#)
 - [Apache mod_ssl Remote Denial of Service \(Updated\)](#)
 - [Apache Mod Proxy Remote Buffer Overflow \(Updated\)](#)
 - [Apache Satisfy Directive Access Control Bypass \(Updated\)](#)
 - [Apple ServerAdmin Default Certificate \(Updated\)](#)
 - [Apple Remote Desktop Administrator Privilege Elevation](#)
 - [Caudium Off-by-One Buffer Overflow](#)
 - [Doug Hanks Sudosh Shell Environment Variable Processing](#)
 - [Free Software Foundation CatDoc XLSView Local Insecure Temporary File Creation](#)
 - [FreeRADIUS Access-Request Denial of Service \(Updated\)](#)
 - [Galeon Browser Tabbed Browsing Spoofing](#)
 - [GD Graphics Library Remote Integer Overflow](#)
 - [Gnome Development Team Epiphany Browser Tabbed Browsing Spoofing](#)
 - [GNU/GPL Samba Buffer Overflow Vulnerabilities \(Updated\)](#)
 - [GNU GetText Insecure Temporary File Creation \(Updated\)](#)
 - [GNU Glibc Insecure Temporary File Creation \(Updated\)](#)
 - [GNU Troff \(Groff\) Insecure Temporary File Creation \(Updated\)](#)
 - [GNU InetUtils TFTP Client Remote Buffer Overflow](#)
 - [ICab Web Browser Cross-Domain Dialog Box Spoofing](#)
 - [ImageMagick Remote EXIF Parsing Buffer Overflow](#)
 - [Kaffeine Media Player Remote Buffer Overflow](#)
 - [KDE Konqueror IFRAME Cross-Domain Scripting](#)
 - [Linux Kernel 64-bit to 32-bit File Offset Conversion Errors Disclose Kernel Memory \(Updated\)](#)
 - [MIT Kerberos 5 Insecure Temporary File Creation \(Updated\)](#)
 - [mixplayd Format String Flaw](#)
 - [Mozilla Bugzilla Multiple Authentication Bypass & Information Disclosure](#)
 - [Mozilla Temporary File Insecure Permissions Information Disclosure](#)
 - [MPG123 Remote URL Open Buffer Overflow \(Updated\)](#)
 - [Multiple Vendors Apache mod_dav Remote Denial of Service \(Updated\)](#)
 - [Multiple Vendors Apache Web Server Remote IPv6 Buffer Overflow \(Updated\)](#)
 - [Multiple Vendors UTempster Multiple Local Vulnerabilities \(Updated\)](#)
 - [Multiple Vendors Zlib Compression Library Remote Denial of Service \(Updated\)](#)
 - [Multiple Vendors Gaim MSNSLP Remote Buffer Overflows \(Updated\)](#)
 - [Multiple Vendors Linux Kernel ReiserFS File System Local Denial of Service](#)
 - [Multiple Vendors LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution \(Updated\)](#)
 - [Multiple Vendors PPPD Remote Denial of Service](#)
 - [Net Integration Technologies Inc. WvTftp Processing TFTP Options Buffer Overflow](#)
 - [NetaTalk Insecure Temporary File Creation \(Updated\)](#)
 - [Omni Group OmniWeb Browser Cross-Domain Dialog Box Spoofing](#)
 - [PHPlist Unspecified Remote Security Vulnerabilities](#)
 - [PNG Development Group Multiple Vulnerabilities in libpng \(Updated\)](#)
 - [PostgreSQL Insecure Temporary File Creation \(Updated\)](#)
 - [QwikMail Format String](#)
 - [HTML::Merge 'printsource.pl' Input Validation](#)
 - [Roaring Penguin Software MIMEDefang Multiple Vulnerabilities](#)
 - [Russell Marks ZGV Image Viewer Multiple Remote Integer Overflow](#)
 - [Ryszard Pydo LinuxStat Remote Directory Traversal](#)
 - [SCO OpenServer Multiple Vulnerabilities in MMDF \(Updated\)](#)
 - [Squid Remote Denial of Service \(Updated\)](#)
 - [Sun StorEdge Sparse File Information Disclosure](#)
 - [Shadow Authentication Bypass](#)
 - [Window Maker WMGLOBAL Font Specification Format String](#)
 - [xmlsoft.org Libxml2 Multiple Remote Stack Buffer Overflows](#)
- Multiple Operating Systems
 - [Hawking Technology HAR11A DSL Router Unauthenticated Administrative Access](#)
 - [Horde Application Framework Help Window Cross-Site Scripting](#)
 - [ID Software Quake II Server Multiple Remote](#)
 - [Land Down Under Input Validation](#)
 - [Mozilla Browser Zombie Document Cross-Site Scripting Vulnerability \(Updated\)](#)
 - [Netscape/Mozilla SOAPParameter Constructor Integer Overflow Vulnerability \(Updated\)](#)
 - [Mozilla / Firefox Certificate Store Corruption Vulnerability \(Updated\)](#)
 - [Mozilla/Firefox/ Thunderbird Multiple Vulnerabilities \(Updated\)](#)

- [Mozilla Multiple Remote Vulnerabilities \(Updated\)](#)
- [Mozilla / Mozilla Firefox "onunload" SSL Certificate Spoofing \(Updated\)](#)
- [Multiple Vendors PuTTY Remote SSH2_MSG_DEBUG Remote Buffer Overflow](#)
- [Multiple Vendor Content Filtering Bypass](#)
- [Multiple Vendor NSS Buffer Overflows \(Updated\)](#)
- [Netcordia Chesapeake TFTP Server Directory Traversal & Remote Denial of Service](#)
- [OpenWFE Remote Cross-Site Scripting & Connection Proxy](#)
- [Phorum Cross-Site Scripting & SQL Injection](#)
- [PHP cURL Open_Basedir Restriction Bypass](#)
- [phpCodeGenie Remote Arbitrary Code Execution](#)
- [PostNuke Trojan Horse](#)
- [Quicksilver Master of Orion III Multiple Remote Denials of Service](#)
- [Raditha Dissanayake Mega Upload Filenames](#)
- [RealPlayer Skin File Buffer Overflow](#)
- [Richard Ellerbrock IPplan Input Validation](#)
- [SKForum 'my wiki' & 'wiki'](#)
- [Stuart Caie cabextract Remote Directory Traversal \(Updated\)](#)
- [Sun Java System Web Proxy Server Multiple Buffer Overflows](#)

[Recent Exploit Scripts/Techniques](#)

[Trends](#)

[Viruses/Trojans](#)

Bugs, Holes, & Patches

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

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

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

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

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Allied Telesyn AT-TFTP Server version 1.8 and prior	A vulnerability exists which could allow a remote malicious user to view or write files on the target system or cause the TFTP service to crash. A remote malicious user can supply a specially crafted filename containing '../' directory traversal characters to view files on or, if 'Read/Write' mode is enabled, upload files to the target system with the privileges of the TFTP service. It is also reported that a remote malicious user can send a filename field that can trigger a buffer overflow and cause the TFTP service to crash. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Allied Telesyn AT-TFTP Server Arbitrary File Execution or Denial of Service	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1012011, October 31, 2004
Apple QuickTime prior to 6.5.2	An integer overflow vulnerability may permit a remote malicious user to execute arbitrary code on the target system. A remote malicious user can create HTML that, when loaded by the target user, will trigger the integer overflow. The vendor has released a fixed version (6.5.2), available at: http://www.apple.com/quicktime/download/ We are not aware of any exploits for this vulnerability.	Apple QuickTime Integer Overflow CVE Name: CAN-2004-0988	High	SecurityTracker Alert ID, 1011969, October 27, 2004
Akella Age of Sail II 1.04.151 and prior versions	A buffer overflow vulnerability may permit a remote malicious user to execute arbitrary code on the target system. A remote user can join a game server and supply a specially crafted nickname to trigger a buffer overflow. No workaround or patch available at time of publishing. Another Proof of Concept exploit script has been published.	Akella Age of Sail II Buffer Overflow	High	Secunia Advisory ID, SA12905, October 21, 2004 Packetstorm, October 27, 2004
Code-Crafters Ability (Mail and FTP) Server 2.3.4	A buffer overflow vulnerability was reported in the Ability Server in the FTP service which could allow a remote authenticated malicious user to execute arbitrary code on the target system. No workaround or patch available at time of publishing. More exploit scripts have been published.	Code-Crafters Ability Server Buffer Overflow	High	Secunia Advisory ID, SA12941, October 25, 2004 SecurityFocus,

				Bugtraq ID 11508, October 22, 2004 Packetstorm, October 27, 2004
Global Spy Software Cyber Web Filter 2.00	A vulnerability exists which can be exploited by malicious people to bypass certain security restrictions. The web filter can be configured to restrict access based on the destination IP address of a website. The vulnerability is caused due to insufficient validation of IP addresses in client requests. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Global Spy Software Cyber Web Filter IP Address Restriction Security Bypass	Medium	Secunia Advisory ID, SA13024, October 29, 2004
Google Google Desktop Search	A remote malicious user can create a specially crafted URL that, when loaded by a target user that has Google Desktop Search installed, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the Google site and will run in the security context of that site. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Google Desktop Search 'meta' Tag Input Validation	High	SecurityTracker Alert ID, 1011928, October 26, 2004
Imspire GSuite	A vulnerability exists that could permit a local malicious user to obtain the target user's GMail password. A local user with access to the target user's 'documents and settings\user_name\Application Data\GSuite' folder can view the 'settings.xml' file, which contains the target user's password in ASCII value encoded form. No workaround or patch available at time of publishing. No exploit is required.	Imspire GSuite Passwords Disclosure	Medium	SecurityTracker Alert ID, 1011994, October 29, 2004
Kingsoft XDICT 2002, 2003, 2004, 2005	A buffer overflow vulnerability exists that could permit a remote malicious user to execute arbitrary code on the target user's computer. When the 'Screen Fetch' mode is enabled and the target user places the mouse over a word that is longer than 88 characters, a buffer overflow will be triggered that may allow a remote malicious user to execute arbitrary code. No workaround or patch available at time of publishing. No exploit is required.	Kingsoft XDICT Word Translation Buffer Overflow	High	SecurityTracker Alert ID, 1012017, November 1, 2004
MailEnable MailEnable Professional prior to version 1.51	A vulnerability with an unknown impact has been reported in MailEnable Professional by the vendor. The vulnerability is caused due to an unspecified error within the webmail functionality. Update to version 1.51: http://www.mailenable.com/download.asp We are not aware of any exploits for this vulnerability.	MailEnable Professional Unspecified Webmail	Low	Secunia Advisory ID, SA13062, November 2, 2004
Microsoft Internet Explorer 6, Microsoft Outlook Express 6	A vulnerability exists which can be exploited by malicious people to trick users into visiting a malicious website by obfuscating URLs. This vulnerability was confirmed in SP1 but not SP2. A Proof of Concept exploit has been published.	Microsoft Internet Explorer/Outlook Express Restricted Zone Status Bar Spoofing	Low	Secunia Advisory ID, SA13015, October 29, 2004
Microsoft Internet Explorer 6.0	Microsoft Internet Explorer is reported prone to a remote Denial of Service vulnerability. The issue presents itself due to a malfunction that occurs when certain font tags are encountered and rendered. When a page that contains the malicious HTML code is viewed, Internet Explorer will crash. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer Font Tag Denial of Service	Low	SecurityFocus Bugtraq ID, 1536, October 26, 2004
Microsoft Internet Explorer 6.0 SP1, Microsoft Internet Explorer 6.0	A remote buffer overflow vulnerability exists due to insufficient boundary checks performed by the application and results in a Denial of Service condition. Arbitrary code execution may be possible as well. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	SecurityFocus, Bugtraq ID 11515, October 25, 2004
Microsoft Internet Explorer 6.0 SP2	A vulnerability exists in the 'hhctrl' Internet Explorer ActiveX control and could allow a malicious user to influence Internet Explorer into running script in the context of a foreign domain. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer HHCtrl ActiveX Control Cross-Domain Scripting	High	SecurityFocus, Bugtraq ID 11521, October 25, 2004
Microsoft Microsoft	A Denial of Service vulnerability was reported in Microsoft Remote Desktop on Windows XP. A remote authenticated malicious user can access the target system and issue the Tsshutdn command to restart a	Microsoft Remote Desktop on Windows XP	Low	SecurityTracker Alert ID, 1011940,

Remote Desktop on Windows XP prior to SP2	Windows XP-based system. The vendor has issued a fix as part of Windows XP SP2. The knowledge base article describing this issue is available at: http://support.microsoft.com/default.aspx?scid=kb;en-us;838202 A Proof of Concept exploit has been published.	Denial of Service		October 26, 2004
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Server, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange 2000 Server, Exchange Server 2003	A remote code execution vulnerability exists within the Network News Transfer Protocol (NNTP) component of the affected operating systems, which could let a remote malicious user execute arbitrary code. This vulnerability could potentially affect systems that do not use NNTP. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-036.msp A Proof of Concept exploit has been published.	Microsoft NNTP Remote Code Execution CVE Name: CAN-2004-0574	High	Microsoft Security Bulletin MS04-036, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 US-CERT Vulnerability Note VU#203126, October 22, 2004 SecurityFocus, Bugtraq ID 11379, October 26, 2004
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	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.msp 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.CSSLv1Detail&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.CSSLv1Detail&executeTransaction=avaya.css.UsageUpdate() 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

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				
Multiple Vendors McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV Archive::Zip 1.13	Remote exploitation of an exceptional condition error in multiple vendors' anti-virus software allows malicious users to bypass security protections by evading virus detection. The problem specifically exists in the parsing of .zip archive headers. This vulnerability affects multiple anti-virus vendors including McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV. Instructions for vendor fixes available at: http://www.odefense.com/application/poi/display?id=153&type=vulnerabilities&flashstatus=true There is no solution for Archive::Zip Proofs of Concept exploits have been published.	Multiple Vendor Anti-Virus Software Detection Evasion CVE Names: CAN-2004-0932 CAN-2004-0933 CAN-2004-0934 CAN-2004-0935 CAN-2004-0936 CAN-2004-0937	High	iDEFENSE Security Advisory, October 18, 2004 Secunia Advisory ID: SA13038, November 1, 2004
Tabs Laboratories MailCarrier 2.51	A buffer overflow vulnerability exists which could allow a remote malicious user to execute arbitrary code on the target system. The flaw resides in the processing of EHLO SMTP commands. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Tabs Laboratories MailCarrier EHLO SMTP Commands Buffer Overflow	High	SecurityFocus Bugtraq ID, 11535, October 26, 2004
Website Pros NetObjects Fusion 8.x	A buffer overflow vulnerability exists, which can be exploited by malicious people to compromise a vulnerable system. Update available at: http://netobjects.com/update/installer/v_0000/NOF8_Update2.exe We are not aware of any exploits for this vulnerability.	Website Pros NetObjects Fusion JPEG Processing Buffer Overflow	High	NetObjects Fusion 8 Product Updates (version 8.00.0000.5030), October 26, 2004

[\[back to top\]](#)

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

	<p>HP: http://software.hp.com</p> <p>We are not aware of any exploits for this vulnerability.</p>			<p>Linux Security Advisory, TSLSA-2004-0047, September 16, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004</p> <p>Fedora Update Notification, FEDORA-2004-313, September 23, 2004</p> <p>HP Security Bulletin, HPSBUX01090, October 26, 2004</p>
<p>Apache Software Foundation</p> <p>Apache 2.0.50</p>	<p>A remote Denial of Service vulnerability exists in 'char_buffer_read()' when using a RewriteRule to reverse proxy SSL connections.</p> <p>Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-463.html</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-21.xml</p> <p>Trustix: http://www.trustix.org/errata/2004/0047/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>HP: http://h30097.www3.hp.com/internet/download.htm</p> <p>There is no exploit code required; however, Proofs of Concept exploits have been published.</p>	<p>Apache mod_ssl Remote Denial of Service</p> <p>CVE Name: CAN-2004-0751</p>	<p>Low</p> <p>SecurityTracker Alert ID, 1011213, September 10, 2004</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2004:096, September 15, 2004</p> <p>RedHat Security Advisory, RHSA-2004:463-09, September 15, 2004</p> <p>Gentoo Linux Security Advisory GLSA 200409-21, September 16, 2004</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2004-0047, September 16, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004</p> <p>Fedora Update Notification, FEDORA-2004-313, September 23, 2004</p> <p>HP Security Bulletin, HPSBUX01090 & HPSBGN01091, October 26 & 29, 2004</p>	
<p>Apache Software Foundation</p> <p>Conectiva</p> <p>Gentoo</p> <p>HP</p> <p>Immunix</p> <p>Mandrake</p> <p>OpenBSD</p> <p>OpenPKG</p>	<p>A buffer overflow vulnerability exists in Apache mod_proxy when a 'ContentLength:' header is submitted that contains a large negative value, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.</p> <p>Patches available at: http://marc.theaimsgroup.com/?l=apache-httpd-dev&m=108687304202140&q=p3</p> <p>OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/</p>	<p>Apache Mod_Proxy Remote Buffer Overflow</p> <p>CVE Name: CAN-2004-0492</p>	<p>Low/High</p> <p>(High if arbitrary code can be executed)</p> <p>SecurityTracker Alert, 1010462, June 10, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200406-16, June 22, 2004</p>	

RedHat SGI Trustix Apache 1.3.26-1.3.29, 1.3.31; OpenBSD –current, 3.4, 3.5	OpenPKG: http://ftp.openpkg.org/release/2.0/UPD/apache-1.3.29-2.0.3.src.rpm Gentoo: http://security.gentoo.org/glsa/glsa-200406-16.xml Mandrake: http://www.mandrakesoft.com/security/advisories SGI: ftp://patches.sgi.com/support/free/security/ Fedora Legacy: http://download.fedoralegacy.org/redhat/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Currently we are not aware of any exploits for this vulnerability.			Mandrakelinux Security Update Advisory, MDKSA-2004:065, June 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.029, June 11, 2004 SGI Security Advisory, 20040605-01-U, June 21, 2004 Fedora Legacy Update Advisory, FLSA:1737, October 14, 2004 US-Cert Vulnerability Note VU#541310, October 19, 2004 Slackware Security Advisory, SSA:2004-299-01, October 26, 2004
Apache Software Foundation Apache 2.0.51	A vulnerability exists in the merging of the 'Satisfy' directive, which could let a remote malicious user obtain access to restricted resources. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-33.xml Trustix: http://http.trustix.org/pub/trustix/updates/ HP: http://h30097.www3.hp.com/internet/download.htm There is no exploit code required.	Apache Satisfy Directive Access Control Bypass CVE Name: CAN-2004-0811	Medium	SecurityFocus, September 24, 2004 HP Security Bulletin, HPSBUX01090 & HPSBGN01091, October 26 & 29, 2004
Apple MacOS X 10.2.8, 10.3.5	A vulnerability exists in ServerAdmin because the same common self-signed certificate is used if the administrator has not replaced this example certificate, which could let a remote malicious user obtain sensitive information. Update available at: http://www.apple.com/support/downloads/ Apple QuickTime: http://www.apple.com/quicktime/download/standalone/ We are not aware of any exploits for this vulnerability.	Apple ServerAdmin Default Certificate CVE Name: CAN-2004-0927	Medium	Apple Security Advisory, SA-2004-09-30, October 4, 2004 Apple Security Advisory, APPLE-SA-2004-10-27, October 27, 2004
Apple Remote Desktop 2.0	A vulnerability exists due to a failure to activate applications with correct privileges, which could let a malicious user obtain superuser privileges. Upgrade available at: http://wsidecar.apple.com/cgi-bin/nph-reg3rdp1.pl/product=04934&platform=osx&method=sa/SecurityUpdate2004-10-27.dmg There is no exploit code required.	Apple Remote Desktop Administrator Privilege Elevation CVE Name: CAN-2004-0962	High	Apple Security Advisory, APPLE-SA-2004-10-27, October 27, 2004
Caudium Caudium 1.2 .x, 1.3 .x, 1.4.1, 1.4.2, 1.4.4 RC1	An off-by-one- buffer overflow vulnerability exists when processing HTTP requests which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code. Upgrades available at: ftp://ftp.us.caudium.net/pub/caudium/source/caudium-1.4.4.tar.gz There is no exploit code required; however, a Proof of Concept exploit has been published.	Caudium Off-by-One Buffer Overflow	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011997, November 1, 2004
Doug Hanks sudosh 1.0, 1.1,	A vulnerability exists in the 'prepchild()' function in 'sudosh.c.' The impact was not specified.	Sudosh Shell Environment Variable Processing	No Specified	SecurityFocus, October 26, 2004

1.2.2, 1.2.3, 1.3, 1.3.2, 1.3.4-1.3.6	<p>Upgrades available at: http://freshmeat.net/redirect/sudosh/53247 /url_tgz/sudosh-1.4.0.tar.gz</p> <p>We are not aware of any exploits for this vulnerability.</p>			
Free Software Foundation CatDoc 0.91.5	<p>A vulnerability exists in 'msxlsview.sh' due to a design error that causes the application to fail to verify the existence of a temporary file prior to writing to it, which could let a remote malicious user corrupt arbitrary files.</p> <p>Debian: http://security.debian.org/pool/updates/main/c/catdoc/</p> <p>There is no exploit code required.</p>	CatDoc XLSView Local Insecure Temporary File Creation CVE Name: CAN-2003-0193	Medium	Debian Security Advisory DSA 575-1, October 28, 2004
FreeRADIUS Server Project FreeRADIUS 0.2-0.5, 0.8, 0.8.1, 0.9-0.9.3, 1.0	<p>A remote Denial of Service vulnerability exists in 'radius.c' and 'eap_tls.c' due to a failure to handle malformed packets.</p> <p>Upgrades available at: ftp://ftp.freeradius.org/pub/radius/freeradius-1.0.1.tar.gz</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-29.xml</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>There is no exploit code required.</p>	FreeRADIUS Access-Request Denial of Service	Low	Gentoo Linux Security Advisory, GLSA 200409-29, September 22, 2004 US-CERT Vulnerability Note VU#541574, October 11, 2004 Fedora Update Notification, FEDORA-2004-355, October 28, 2004
Galeon Galeon Browser 1.3.18	<p>A vulnerability exists in the tabbed browsing feature, which could let a remote malicious user spoof web page functions.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	Galeon Browser Tabbed Browsing Spoofing	Medium	SecurityTracker Alert ID, 1012002, October 30, 2004
GD Graphics Library gdlib 2.0.23, 2.0.26-2.0.28	<p>A vulnerability exists in the 'gdImageCreateFromPngCtx()' function when processing PNG images due to insufficient sanity checking on size values, which could let a remote malicious user execute arbitrary code.</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/</p> <p>An exploit script has been published.</p>	GD Graphics Library Remote Integer Overflow CVE Name: CAN-2004-0990	High	Secunia Advisory, SA12996, October 28, 2004
Gnome Development Team Epiphany Browser 1.4.4	<p>A vulnerability exists in the tabbed browsing feature, which could let a remote malicious user spoof web page functions.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	Epiphany Browser Tabbed Browsing Spoofing	Medium	SecurityTracker Alert ID, 1012003, October 30, 2004
GNU / GPL Conectiva Gentoo Mandrake RedHat SuSE Trustix Samba 3.0.0 - 3.0.4 and 2.2.9 and prior	<p>Multiple buffer overflow vulnerabilities exist in Samba that could allow a remote user to execute arbitrary code on the target system. These are caused by boundary errors when decoding base64 data and when handling 'mangling method = hash.'</p> <p>Upgrade to version 3.0.5 or 2.2.10 available at: http://us2.samba.org/samba/ftp/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br</p> <p>RedHat: RedHat Enterprise Linux AS 3, ES 3, WS 3: http://rhn.redhat.com/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200407-21.xml</p> <p>Mandrakesoft: Mandrake Multi Network Firewall 8.x, 9.x; Mandrake Corporate Server 2.x http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:071</p> <p>SuSE: SuSE Linux, Email, Database, and Enterprise Servers http://www.suse.de/de/security/2004_22_samba.html</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57664-1&searchclause=</p> <p>A working exploit has been published.</p>	Samba Buffer Overflow Vulnerabilities CVE Names: CAN-2004-0600 CAN-2004-0686	High	Samba Release Notes 3.0.5, July 20, 2004 Gentoo, RedHat, Mandrakesoft, SuSE, Trustix, Conectiva Advisories Sun(sm) Alert Notification, 57664, October 25, 2004
GNU gettext 0.14.1	<p>A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files.</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p>	GNU GetText Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050,

	<p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-10.xml</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gettext/</p> <p>There is no exploit code required.</p>	<p>CVE Name: CAN-2004-0966</p>	<p>September 30, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200410-10, October 10, 2004</p> <p>Ubuntu Security Notice, USN-5-1 October 27, 2004</p>
<p>GNU</p> <p>glibc 2.0-2.0.6, 2.1, 2.1.1 -6, 2.1.1, 2.1.2, 2.1.3 -10, 2.1.3, 2.1.9 & greater, 2.2-2.2.5, 2.3-2.3.4, 2.3.10</p>	<p>A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files.</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-19.xml</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/glibc/</p> <p>There is no exploit code required.</p>	<p>GNU</p> <p>Glibc Insecure Temporary File Creation</p> <p>CVE Name: CAN-2004-0968</p>	<p>Medium</p> <p>Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200410-19, October 21, 2004</p> <p>Ubuntu Security Notice, USN-4-1 October 27, 2004</p>
<p>GNU</p> <p>groff 1.19</p>	<p>A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files.</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/groff/</p> <p>There is no exploit code required.</p>	<p>GNU Troff (Groff)</p> <p>Insecure Temporary File Creation</p> <p>CVE Name: CAN-2004-0969</p>	<p>Medium</p> <p>Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004</p> <p>Ubuntu Security Notice USN-13-1, November 1, 2004</p>
<p>GNU</p> <p>InetUtils 1.4.2</p>	<p>A buffer overflow vulnerability exists in 'main.c' due to boundary errors when handling DNS responses, which could let a remote malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>GNU InetUtils TFTP Client Remote Buffer Overflow</p>	<p>High</p> <p>Bugtraq, October 26, 2004</p>
<p>iCab Company</p> <p>iCab 2.9.8</p>	<p>A cross-domain dialog box spoofing vulnerability exists which could let a remote malicious user spoof an interface of a trusted web site.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>iCab Web Browser Cross-Domain Dialog Box Spoofing</p>	<p>Medium</p> <p>Secunia Advisory, SA12982, October 26, 2004</p>
<p>ImageMagick</p> <p>ImageMagick 5.3.3, 5.4.3, 5.4.4.5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0, 6.0.1, 6.0.3-6.0.8</p>	<p>A buffer overflow vulnerability exists in the 'EXIF' parsing routine due to a boundary error, which could let a remote malicious user execute arbitrary code.</p> <p>Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=24099</p> <p>Redhat: http://rhn.redhat.com/errata/RHSA-2004-480.html</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>ImageMagick Remote EXIF Parsing Buffer Overflow</p> <p>CVE Name: CAN-2004-0981</p>	<p>High</p> <p>SecurityTracker Alert ID, 1011946, October 26, 2004</p>
<p>Kaffeine</p> <p>Media Player 0.4.2, 0.4.3 b, 0.4.3, 0.5 rc1</p>	<p>A buffer overflow vulnerability exists in the processing of Content-Type headers in the 'http_open()' function in 'http.c' due to insufficient boundary checks on user-supplied strings prior to copying them into finite stack-based buffers, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	<p>Kaffeine Media Player Remote Buffer Overflow</p>	<p>Low/High</p> <p>(High if arbitrary code can be executed)</p> <p>Securiteam, October 26, 2004</p>
<p>KDE</p> <p>Konqueror 3.1.4, 3.2.1, 3.2.2 -6</p>	<p>A cross-domain scripting vulnerability exists due to a failure to prevent JavaScript that is rendered in one frame from accessing properties of a site contained in an alternate frame, which could let a remote malicious web site render JavaScript in the context of an alternate domain.</p> <p>This has been addressed in KDE Konqueror version 3.2.3.</p> <p>A Proof of Concept exploit has been published.</p>	<p>KDE Konqueror IFRAME Cross-Domain Scripting</p>	<p>Medium</p> <p>SecurityFocus, October 27, 2004</p>

Linux Fedora RedHat SuSE Linux kernel 2.4 through 2.4.26, 2.6 through 2.6.7	<p>A vulnerability exists in the Linux kernel in the processing of 64-bit file offset pointers thus allowing a local malicious user to view kernel memory. The kernel's file handling API does not properly convert 64-bit file offsets to 32-bit file offsets. In addition, the kernel provides insecure access to the file offset member variable. As a result, a local user can gain read access to large portions of kernel memory.</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>RedHat: http://rhn.redhat.com/</p> <p>SuSE: http://www.suse.de/de/security/2004_24_kernel.html</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-24.xml</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>A Proof of Concept exploit script has been published.</p>	Linux Kernel 64-bit to 32-bit File Offset Conversion Errors Disclose Kernel Memory CVE Name: CAN-2004-0415	High	<p>ISEC Security Research, August 4, 2004</p> <p>SGI Security Advisory, 20040804-01-U, August 26, 2004</p> <p>Gentoo Linux Security Advisory GLSA 200408-24, August 25, 2004</p> <p>Mandrakelinux Security Update Advisory, August 26, 2004</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2004-0041, August 9, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:879, October 26, 2004</p>
MIT Kerberos 5 1.3.4	<p>A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files.</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-24.xml</p> <p>There is no exploit code required.</p>	MIT Kerberos 5 Insecure Temporary File Creation CVE Name: CAN-2004-0971	Medium	<p>Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004</p> <p>Gentoo Linux Security Advisory GLSA 200410-24, October 25, 2004</p>
mixplayd mixplayd 0.53	<p>A format string vulnerability exists in 'main.c' because data is printed without proper format specifiers, which could let a remote malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>We are not aware of any exploits for this vulnerability.</p>	mixplayd Format String Flaw	High	Zone-h Security Advisory, ZH2004-17SA, October 29, 2004
Mozilla.org Bugzilla 2.4, 2.6, 2.8, 2.10, 2.12, 2.14-2.14.5, 2.16-2.16.5, 2.17-2.17.7, 2.18 rc1&rc2	<p>Multiple vulnerabilities exist: a vulnerability exists in 'process_bug.cgi' when a specially crafted HTTP POST request to remove keywords from a bug is submitted, which could let a remote malicious user obtain sensitive information; a vulnerability exists when exporting bugs to XML, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because various private attachment metadata is disclosed, which could let a remote malicious user see private attachments.</p> <p>Upgrades available at: http://www.bugzilla.org/download/</p> <p>There is no exploit code required.</p>	Mozilla Bugzilla Multiple Authentication Bypass& Information Disclosure	Medium	Bugzilla Security Advisory, October 24, 2004
Mozilla.org Mozilla Browser 1.7, rc1-rc3, beta, alpha, 1.7.1-1.7.3, 1.8 Alpha 1-4, Firefox Preview Release Mozilla Firefox 0.9, rc, 0.9.1-0.9.3, 0.10, 0.10.1, Thunderbird 0.6, 0.7-0.7.3, 0.8	<p>A vulnerability exists in the 'Open with' option because the software saves the file in the '/tmp' directory with world-readable permissions, which could let a malicious user obtain sensitive information.</p> <p>Fixes are available in the CVS repository.</p> <p>There is no exploit code required.</p>	Mozilla Temporary File Insecure Permissions Information Disclosure	Medium	Secunia Advisory, SA12956, October 25, 2004
mpg123.de mpg123 pre0.59s, 0.59r	<p>A buffer overflow vulnerability exists in the 'getauthfromURL()' function due to a boundary error, which could let a remote malicious user execute arbitrary code.</p> <p>Debian: http://security.debian.org/pool/updates/non-free/m/mpg123/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-27.xml</p> <p>A Proof of Concept exploit has been published.</p>	MPG123 Remote URL Open Buffer Overflow CVE Name: CAN-2004-0982	High	<p>Securiteam, October 21, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200410-27, October 27, 2004</p> <p>Debian Security</p>

				Advisory, DSA 578-1 , November 1, 2004
Multiple Vendors Apache Software Foundation Apache 2.0.50 & prior; Gentoo Linux 1.4; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A remote Denial of Service vulnerability exists in the Apache mod_dav module when an authorized malicious user submits a specific sequence of LOCK requests. Update available at: http://httpd.apache.org/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml RedHat: ftp://updates.redhat.com/enterprise Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/liba/ HP: http://software.hp.com There is no exploit code required; however, a Proof of Concept exploit has been published.	Apache mod_dav Remote Denial of Service CVE Name: CAN-2004-0809	Low	SecurityTracker Alert ID, 1011248, September 14, 2004 Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004 Fedora Update Notification, FEDORA-2004-313, September 23, 2004 Debian Security Advisory DSA 558-1 , October 6, 2004 HP Security Bulletin, HPSBUX01090, October 26, 2004
Multiple Vendors Apache Software Foundation Apache 2.0.50 & prior; Gentoo Linux 1.4; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core1&2; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1; Turbolinux Turbolinux Desktop 10.0	A buffer overflow vulnerability exists in the apr-util library's IPv6 URI parsing functionality due to insufficient validation, which could let a remote malicious user execute arbitrary code. <i>Note: On Linux based Unix variants this issue can only be exploited to trigger a Denial of Service condition.</i> Patch available at: http://www.apache.org/dist/httpd/patches/apply_to_2.0.50/CAN-2004-0747.patch Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Redhat: http://rhn.redhat.com/errata/RHSA-2004-463.html http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Turbolinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ HP: http://h30097.www3.hp.com/internet/download.htm We are not aware of any exploits for this vulnerability.	Apache Web Server Remote IPv6 Buffer Overflow CVE Name: CAN-2004-0786	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 16, 2004 Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004 Fedora Update Notifications, FEDORA-2004-307 & 308, September 16, 2004 HP Security Bulletin, HPSBUX01090 & HPSBGN01091, October 26 & 29, 2004
Multiple Vendors Fedora Mandrake Slackware RedHat SGI Slackware Linux – current, 9.1; utempter utempter 0.5.2, 0.5.3	Multiple vulnerabilities exist: a vulnerability exists due to an input validation error that causes the application to exit improperly, which could let a malicious user obtain root privileges; and a vulnerability exists due to a failure to validate buffer boundaries, which could let a malicious user cause a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/l/utempter-1.1.1-i486-1.tgz RedHat: ftp://updates.redhat.com/9/en/os/SRPMS/utempter-0.5.5-2.RHL9.0.src.rpm SGI: http://www.sgi.com/support/security/ Sun: http://sunsolve.sun.com/search/	UTempter Multiple Local Vulnerabilities CVE Name: CAN-2004-0233	Low/High (Low if a DoS; and High if root privileges can be obtained)	Fedora Update Notification, FEDORA-2004-108, April 21, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:031-1, April 21, 2004 Slackware Security Advisory, SSA:2004-110-01, April 19, 2004 Red Hat Security Advisory, RHSA-

	<p>document.do?assetkey=1-26-57658-1&searchclause</p> <p>A Proof of Concept exploit has been published.</p>			<p>2004:175-01, April 30, 2004</p> <p>SGI Security Advisories, 20040602-01-U & 20040603-01-U, June 21, 2004</p> <p>Sun(sm) Alert Notification, 57658, October 26, 2004</p>
<p>Multiple Vendors</p> <p>FileZilla Server 0.7, 0.7.1; OpenBSD - current, 3.5; OpenPKG Current, 2.0, 2.1; zlib 1.2.1</p>	<p>A remote Denial of Service vulnerability during the decompression process due to a failure to handle malformed input.</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-26.xml</p> <p>FileZilla: http://sourceforge.net/project/showfiles.php?group_id=21558</p> <p>OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/017_libz_patch</p> <p>OpenPKG: ftp://ftp.openpkg.org</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.17</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Zlib Compression Library Remote Denial of Service</p> <p>CVE Name: CAN-2004-0797</p>	<p>Low</p> <p>SecurityFocus, August 25, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:029, September 2, 2004</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2004:090, September 8, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:865, September 13, 2004</p> <p>US-CERT Vulnerability Note VU#238678, October 1, 2004</p> <p>SCO Security Advisory, SCOSA-2004.17, October 19, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:878, October 25, 2004</p>	
<p>Multiple Vendors</p> <p>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</p>	<p>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.</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-23.xml</p> <p>Rob Flynn: http://prdownloads.sourceforge.net/gaim/gaim-1.0.2.tar.gz?download</p> <p>RedHat: ftp://updates.redhat.com</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.0/patches/packages/gaim-1.0.2-i486-1.tgz</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Gaim MSNSLP Remote Buffer Overflow</p> <p>CVE Name: CAN-2004-0891</p>	<p>High</p> <p>Gentoo Linux Security Advisory, GLSA 200410-23, October 25, 2004</p> <p>RedHat Security Advisory, RHSA-2004:604-01, October 20, 2004</p> <p>Slackware Security Advisory, SSA:2004-296-01, October 22, 2004</p> <p>Ubuntu Security Notice, USN-8-1 October 27, 2004</p>	
<p>Multiple Vendors</p> <p>Linux kernel 2.6.8 rc1-rc3</p>	<p>A Denial of Service vulnerability exists in the 'ReiserFS' file system functionality due to a failure to properly handle files under certain conditions.</p> <p>Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.9.tar.bz2</p>	<p>Linux Kernel ReiserFS File System Local Denial of Service</p> <p>CVE Name:</p>	<p>Low</p> <p>SecurityFocus, October 26, 2004</p>	

	There is no exploit code required.	CAN-2004-0814		
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/ We are not aware of any exploits for this vulnerability.	LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution CVE Name: CAN-2004-0801	High	Secunia Advisory, SA12557, September 16, 2004 Fedora Update Notification, FEDORA-2004-303, September 21, 2004 Gentoo Linux Security Advisory, GLSA 200409-24, September 17, 2004 Sun(sm) Alert Notification, 57646, October 7, 2004 Conectiva Linux Security Announcement, CLA-2004:880, October 26, 2004
Multiple Vendors Paul Mackerras PPPD 2.4.1; Ubuntu Ubuntu Linux 4.1 ppc, ia64, ia32	A remote Denial of Service vulnerability exists in the 'cbcp_input()' function, due to a failure to properly handle invalid input. Upgrade available at: http://security.ubuntu.com/ubuntu/pool/main/p/ppp/ We are not aware of any exploits for this vulnerability.	PPPD Remote Denial of Service	Low	Bugtraq, October 26, 2004
Net Integration Technologies Inc. WvTftp 0.9	A buffer overflow vulnerability exists in the 'WvTFTPServer::new_connection()' function in 'wvftpsrvr.cc' due to a insufficient sanity checking, which could let a remote malicious user execute arbitrary code with root privileges. No workaround or patch available at time of publishing. An exploit script has been published.	WvTftp Processing TFTP Options Buffer Overflow	High	Bugtraq, October 26, 2004
Netatalk Netatalk Open Source Apple File Share Protocol Suite 1.5 pre6, 1.6.1, 1.6.4	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-200410-25.xml There is no exploit code required.	NetaTalk Insecure Temporary File Creation CVE Name: CAN-2004-0974	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory GLSA 200410-25, October 25, 2004
Omni Group OmniWeb 5.0.1	A cross-domain dialog box spoofing vulnerability exists, which could let a remote malicious user spoof an interface of a trusted web site. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Omni Group OmniWeb Browser Cross-Domain Dialog Box Spoofing	Medium	Secunia Advisory, SA13002, October 27, 2004
phplist.com Mailing List Manager 2.6-2.6.3	Some security vulnerabilities exist in PHPlist. The impact was not specified. Update available at: http://sourceforge.net/project/showfiles.php?group_id=91074 We are not aware of any exploits for this vulnerability.	PHPlist Unspecified Remote Security Vulnerabilities	Not Specified	SecurityTracker Alert ID: 1011958, October 27, 2004
PNG Development Group Conectiva Debian Fedora Gentoo Mandrakesoft RedHat SuSE Sun Solaris HP-UX GraphicsMagick ImageMagick Slackware	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: <ul style="list-style-type: none">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/	Multiple Vulnerabilities in libpng CVE Names: CAN-2004-0597 CAN-2004-0598 CAN-2004-0599	High	US-CERT Technical Cyber Security Alert TA04-217A, August 4, 2004 US-CERT Vulnerability Notes VU#160448, VU#388984, VU#817368, VU#236656, VU#477512, VU#286464,

libpng 1.2.5 and 1.0.15	<p>index.php?id=a&anuncio=000856</p> <p>Debian: http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00139.html</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-03.xml</p> <p>Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:079</p> <p>RedHat http://rhn.redhat.com/</p> <p>SuSE: http://www.suse.de/de/security/2004_23_libpng.html</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>Sun Solaris: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert/57617</p> <p>HP-UX: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01065</p> <p>GraphicsMagick: http://www.graphicsmagick.org/www/download.html</p> <p>ImageMagick: http://www.imagemagick.org/www/download.html</p> <p>Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.439243</p> <p>Yahoo: http://messenger.yahoo.com/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse</p> <p>SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.16</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>A Proof of Concept exploit has been published.</p>			<p>August 4, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:035, October 5, 2004</p> <p>SCO Security Advisory, SCOSA-2004.16, October 12, 2004</p> <p>Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004</p>
PostgreSQL PostgreSQL 7.4.5	<p>A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files.</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-16.xml</p> <p>Debian: http://security.debian.org/pool/updates/main/p/postgresql/</p> <p>OpenPKG: ftp://ftp.openpkg.org/release/</p> <p>There is no exploit code required.</p>	PostgreSQL Insecure Temporary File Creation CVE Name: CAN-2004-0977	Medium	<p>Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200410-16, October 18, 2004</p> <p>Debian Security Advisory, DSA 577-1, October 29, 2004</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2004.046, October 29, 2004</p>
Qwikmail Qwikmail 0.3	<p>A vulnerability exists due to a format string error in 'qwik-smtpd.c,' which could let a remote malicious user execute arbitrary code.</p> <p>Patch available at: http://qwikmail.sourceforge.net/smtpd/qwik-smtpd-0.3.patch</p> <p>We are not aware of any exploits for this vulnerability.</p>	QwikMail Format String	High	Secunia Advisory, SA13037, November 1, 2004
rmerge.sourceforge.net HTML::Merge 3.0 - 3.42	<p>A vulnerability exists in 'printsource.pl' due to insufficient validation of the 'template' parameter, which could let a remote malicious user execute arbitrary code.</p> <p>Update available at: http://sourceforge.net/project/showfiles.php?group_id=47854</p> <p>We are not aware of any exploits for this vulnerability.</p>	HTML::Merge 'printsource.pl' Input Validation	High	Secunia Advisory, SA13041, November 1, 2004
Roaring Penguin Software	Multiple vulnerabilities exists due to insufficient validation of I/O operations in 'mimedefang.pl.in' and an unspecified input validation error exists in 'mimedefang.c.' The impact was not specified.	Roaring Penguin Software MIMEDefang Multiple Vulnerabilities	Not Specified	SecurityTracker Alert ID, 1011996,

MIMEdefang 2.4, 2.14, 2.20, 2.21, 2.38, 2.39, 2.41-4.47	Upgrades available at: http://www.mimedefang.org/static/mimedefang-2.48.tar.gz We are not aware of any exploits for this vulnerability.			October 29, 2004
Russell Marks zgv Image Viewer 5.5	Several vulnerabilities exist due to various integer overflows when processing images, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	ZGV Image Viewer Multiple Remote Integer Overflow	High	Bugtraq, October 26, 2004
Ryszard Pydo LinuxStat 2.0-2.3	A Directory Traversal vulnerability exists in the 'template' parameter due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information. Update available at: http://sourceforge.net/project/showfiles.php?group_id=38678 There is no exploit code required; however, a Proof of Concept exploit has been published.	Ryszard Pydo LinuxStat Remote Directory Traversal	Medium	Secunia Advisory, SA12963, October 25, 2004
SCO Group SCO OpenServer 5.x	Multiple vulnerabilities exist in SCO MMDF. According to SCO the vulnerabilities are: buffer overflows, null dereferences and core dumps. One of the buffer overflows is known to affect 'execmail.' Updates available at: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2004.7/ An exploit script has been published.	SCO OpenServer Multiple Vulnerabilities in MMDF CVE Names: CAN-2004-0510 CAN-2004-0511 CAN-2004-0512	Medium	SCO Advisory, SCOSA-2004.7, July 14, 2004 Deprotect Security Advisory 20040206, July 2, 2004 PacketStorm October 26, 2004
Squid-cache.org Squid 2.5-STABLE6, 3.0-PRE3-20040702; when compiled with SNMP support	A remote Denial of Service vulnerability exists in the 'asn_parse_header()' function in 'snmplib/asn1.c' due to an input validation error when handling certain negative length fields. Updates available at: http://www.squid-cache.org/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-15.xml Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-591.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/s/squid/ OpenPKG: ftp://ftp.openpkg.org/release/ We are not aware of any exploits for this vulnerability.	Squid Remote Denial of Service CVE Name: CAN-2004-0918	Low	DEFENSE Security Advisory, October 11, 2004 Fedora Update Notification, FEDORA-2004-338, October 13, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-15, October 18, 2004 RedHat Security Advisory, RHSA-2004:591-04, October 20, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:112, October 21, 2004 Debian Security Advisory, DSA 576-1, October 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.048, October 29, 2004
Sun Microsystems, Inc.	A vulnerability exists in StorEdge QFS and SAM-FS, which could let a remote malicious user obtain sensitive information.	Sun StorEdge Sparse File Information Disclosure	Medium	SecurityFocus, October 27, 2004

Performance Suite 4.0, 4.1, Utilization Suite 4.0, 4.1	Workaround available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57595-1&searchclause= There is no exploit code required.			
Tomasz Kloczko Shadow 4.0-4.0.4	A vulnerability exists in the 'chfn' and 'chsh' utilities due to insufficient sanitization of user-supplied input, which could let a remote malicious user bypass authentication. Upgrades available at : ftp://ftp.pld.org.pl/software/shadow/shadow-4.0.5.tar.gz We are not aware of any exploits for this vulnerability.	Shadow Authentication Bypass	Medium	SecurityFocus, October 28, 2004
Windowmaker.org Windowmaker 0.20.1 -3, 0.52 -2, 0.53, 0.60, 0.61, 0.61.1, 0.62, 0.62.1, 0.63, 0.63.1, 0.64, 0.65, 0.65.1, 0.80, 0.80.2	A format string vulnerability exists in the 'WMGLOBAL' configuration file related to the validation of font specifications, which could let a malicious user execute arbitrary code. Upgrades available at: ftp://windowmaker.org/pub/source/release/WindowMaker-0.90.0.tar.gz We are not aware of any exploits for this vulnerability.	Window Maker WMGLOBAL Font Specification Format String	High	SecurityFocus, October 26, 2004
xmlsoft.org Libxml2 2.6.12-2.6.14	Multiple buffer overflow vulnerabilities exist: a vulnerability exists in the 'xmlNanoFTPScanURL()' function in 'nanoftp.c' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'xmlNanoFTPScanProxy()' function in 'nanoftp.c,' which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handling of DNS replies due to various boundary errors, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://xmlsoft.org/sources/libxml2-2.6.15.tar.gz OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ An exploit script has been published.	Libxml2 Multiple Remote Stack Buffer Overflows CVE Name: CAN-2004-0989	High	SecurityTracker Alert 1, : 1011941, October 28, 2004

[\[back to top\]](#)

Multiple Operating Systems - Windows / UNIX / Linux / Other				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Hawking Technology HAR11A DSL Router	A vulnerability exists due to a failure to require authentication credentials prior to allowing administrative access to the devices CLI interface, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	Hawking Technology HAR11A DSL Router Unauthenticated Administrative Access	High	Bugtraq, October 26, 2004
Horde Project Horde 2.0, 2.1, 2.1.3, 2.2, 2.2.1, 2.2.3, 2.2.4, RC1, 2.2.5, 2.2.6	A Cross-Site Scripting vulnerability exists in the 'Help' window due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/horde/horde-2.2.7.tar.gz There is no exploit code required.	Horde Application Framework Help Window Cross-Site Scripting	High	SecurityTracker Alert ID, 1011959, October 27, 2004
id Software, Inc. Quake II Server 3.20, 3.21	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when handling 'Configstrings' and 'Baselines' due to an input validation error; a buffer overflow vulnerability exists when parsing command packets, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists when requesting missing files such as maps from a server running Windows, which could let a remote malicious user download sensitive files; a remote Denial of Service vulnerability exists due to an input validation error when requesting missing files from a Linux server; a vulnerability exists due to an error in the handling of userinfo, which could let a remote malicious user spoof the client's IP address; and a remote Denial of Service vulnerability exists when a malicious user continuously submits multiple join requests. No workaround or patch available at time of publishing. We are not aware of any exploits for these vulnerabilities.	ID Software Quake II Server Multiple Remote	Low/Medium/ High (Low if a DoS: Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	Bugtraq, October 27, 2004
idu.neocrome.net Land Down Under 701	Multiple input validation vulnerabilities exist due to insufficient validation of user-supplied input in several variables, which could let a remote malicious user obtain sensitive information. Update available at: http://www.neocrome.net/index.php?msingle&id91 Proofs of Concept exploits have been published.	Land Down Under Input Validation	Medium	SecurityTracker Alert ID, 1012015, November 1, 2004
Mozilla.org	A Cross-Site Scripting vulnerability exists in 'nsDOMClassInfo.cpp' and occurs when a large number of event handlers are used within HTML tags, which could	Mozilla Browser Zombie Document	High	SecurityFocus, February 25,

<p>Mozilla Browser 0.8, 0.9.2.1, 0.9.2- 0.9.9, 0.9.35, 0.9.48, 1.0, RC1& RC2, 1.0.1, 1.0.2, 1.1- 1.5</p>	<p>let a remote malicious user execute arbitrary code.</p> <p>The vulnerability has been fixed in versions 1.6b and 1.4.2 available at: http://www.mozilla.org/</p> <p>HP: http://www.hp.com/products1/unix/java/mozilla/index.html</p> <p>Redhat: http://rhn.redhat.com/errata/RHSA-2004-110.html</p> <p>SGI: ftp://patches.sgi.com/support/free/security/patches/</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Cross-Site Scripting Vulnerability</p> <p>CVE Name: CAN-2004-0191</p>		<p>2004</p> <p>Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004</p>
<p>Mozilla.org</p> <p>Mozilla 1.6 & prior; Netscape 7.0, 7.1, and prior</p>	<p>A input validation vulnerability exists in the SOAPParameter object constructor in Netscape and Mozilla which allows execution of arbitrary code. The SOAPParameter object's constructor contains an integer overflow that allows controllable heap corruption. A web page can be constructed to leverage this into remote execution of arbitrary code.</p> <p>Upgrade to Mozilla 1.7.1 available at: http://www.mozilla.org/products/mozilla1.x/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Netscape/Mozilla SOAPParameter Constructor Integer Overflow Vulnerability</p> <p>CVE Name: CAN-2004-0722</p>	<p>High</p>	<p>DEFENSE Security Advisory, August 2, 2004</p> <p>Bugzilla Bug 236618</p> <p>SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:877, October 22, 2004</p> <p>Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004</p>
<p>Mozilla.org</p> <p>Mozilla 1.6; Mozilla 1.7.x; Mozilla Firefox 0.x</p>	<p>A Denial of Service vulnerability exists in which arbitrary root certificates are imported silently without presenting users with a import dialog box. Due to another problem, this can e.g. be exploited by malicious websites or HTML-based emails to prevent users from accessing valid SSL sites.</p> <p>Workaround: Check the certificate store and delete untrusted certificates if an error message is displayed with error code -8182 ("certificate presented by [domain] is invalid or corrupt") when attempting to access a SSL-based website.</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>Currently, we are not aware of any exploits for this vulnerability.</p>	<p>Mozilla / Firefox Certificate Store Corruption Vulnerability</p> <p>CVE Name: CAN-2004-0758</p>	<p>Low</p>	<p>Secunia Advisory, SA12076, July 16, 2004</p> <p>Bugzilla Bug 24900, July 14, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:877, October 22, 2004</p> <p>Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004</p>
<p>Mozilla.org Mandrakesoft Slackware</p> <p>Mozilla 1.7 and prior; Firefox 0.9 and prior; Thunderbird 0.7 and prior</p>	<p>Multiple vulnerabilities exist in Mozilla, Firefox, and Thunderbird that could allow a malicious user to conduct spoofing attacks, compromise a vulnerable system, or cause a Denial of Service. These vulnerabilities include buffer overflow, input verification, insecure certificate name matching, and out-of-bounds reads.</p> <p>Upgrade to the latest version of Mozilla, Firefox, or Thunderbird available at: http://www.mozilla.org/download.html</p> <p>Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.667659</p> <p>Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:082</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-421.html</p> <p>SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/</p>	<p>Mozilla/Firefox/Thunderbird Multiple Vulnerabilities</p> <p>CVE Name: CAN-2004-0757 CAN-2004-0759 CAN-2004-0761 CAN-2004-0765</p>	<p>High</p>	<p>Secunia, SA10856, August 4, 2004</p> <p>US-CERT Vulnerability Note VU#561022</p> <p>RedHat Security Advisory, RHSA-2004:421-17, August 4, 2004</p> <p>SGI Security Advisory, 20040802-01-U, August 14, 2004</p> <p>Gentoo Linux</p>

	<p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-26.xml</p> <p>HP: http://h30097.www3.hp.com/internet/download.htm</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>We are not aware of any exploits for these vulnerabilities.</p>			<p>Security Advisory, GLSA 200409-26, September 20, 2004</p> <p>HP Security Bulletin, HPSBTU01081, October 5, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:877, October 22, 2004</p> <p>Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004</p>
<p>Mozilla.org</p> <p>Mozilla 0.x, 1.0-1.7.x, Firefox 0.x, Thunderbird 0.x; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2</p>	<p>Multiple vulnerabilities exist: buffer overflow vulnerabilities exist in 'nsMsgCompUtils.cpp' when a specially crafted e-mail is forwarded, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient restrictions on script generated events, which could let a remote malicious user obtain sensitive information; a buffer overflow vulnerability exists in the 'nsVCardObj.cpp' file due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'nsPop3Protocol.cpp' due to boundary errors, which could let a remote malicious user execute arbitrary code; a heap overflow vulnerability exists when handling non-ASCII characters in URLs, which could let a remote malicious user execute arbitrary code; multiple integer overflow vulnerabilities exist in the image parsing routines due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a cross-domain scripting vulnerability exists because URI links dragged from one browser window and dropped into another browser window will bypass same-origin policy security checks, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because unsafe scripting operations are permitted, which could let a remote malicious user manipulate information displayed in the security dialog.</p> <p>Updates available at: http://www.mozilla.org/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-26.xml</p> <p>HP: http://h30097.www3.hp.com/internet/download.htm</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-486.html</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>Proofs of Concept exploits have been published.</p>	<p>Mozilla Multiple Remote Vulnerabilities</p> <p>CVE Names: CAN-2004-0902 CAN-2004-0903 CAN-2004-0904 CAN-2004-0905 CAN-2004-0908</p>	<p>Medium/ High (High if arbitrary code can be executed)</p>	<p>Technical Cyber Security Alert TA04-261A, September 17, 2004</p> <p>US-CERT Vulnerability Notes VU#414240, VU#847200, VU#808216, VU#125776, VU#327560, VU#651928, VU#460528, VU#113192, September 17, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200409-26, September 20, 2004</p> <p>RedHat Security Bulletin, RHSA-2004:486-18, September 30, 2004</p> <p>HP Security Bulletin, HPSBTU01081, October 5, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:877, October 22, 2004</p> <p>Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004</p>
<p>Mozilla.org</p> <p>Mozilla Firefox 0.9.2</p>	<p>A spoofing vulnerability exists that could allow malicious sites to abuse SSL certificates of other sites. An attacker could make the browser load a valid certificate from a trusted website by using a specially crafted "onunload" event.</p>	<p>Mozilla / Mozilla Firefox "onunload" SSL Certificate</p>	<p>Medium</p>	<p>Cipher.org, July 25, 2004</p>

<p>and Mozilla 1.7.1 on Windows</p> <p>Mozilla Firefox 0.9.2 on Linux</p>	<p>The problem is that Mozilla loads the certificate from a trusted website and shows the "secure padlock" while actually displaying the content of the malicious website. The URL shown in the address bar correctly reads that of the malicious website.</p> <p>An additional cause has been noted due to Mozilla not restricting websites from including arbitrary, remote XUL (XML User Interface Language) files.</p> <p>Workaround: Do not follow links from untrusted websites and verify the correct URL in the address bar with the one in the SSL certificate.</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>A Proof of Concept exploit has been published.</p>	<p>Spoofting</p> <p>CVE Name: CAN-2004-0763</p>		<p>Secunia, SA12160, July 26, 2004; SA12180, July 30, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:877, October 22, 2004</p> <p>Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004</p>
<p>Multiple Vendors</p> <p>Simon Tatham PuTTY 0.48- 0.55; TortoiseCVS TortoiseCVS 1.8</p>	<p>A buffer overflow vulnerability exists in the 'ssh2_rdpkt()' function due to insufficient validation of the string length parameter in 'SSH2_MSG_DEBUG' packets, which could let a remote malicious user execute arbitrary code.</p> <p>Simon Tatham: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html</p> <p>Tortoise: http://prdownloads.sourceforge.net/tortoise/tortoiseCVS-1.8.3.exe?download</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-29.xml</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>PuTTY Remote SSH2_MSG_DEBUG Remote Buffer Overflow</p>	<p>High</p>	<p>iDefense Security Advisory, October 27, 2004</p>
<p>Multiple Vendors</p> <p>Agnum Outpost Firewall 2.1, 2.5; ATGuard ATGuard Personal Firewall 3.2; Check Point Software FireWall-1 Next Generation FP0-FP3, VPN-1 Next Generation FP0-FP2; Internet Security Systems BlackICE PC Protection 3.6 cch, ccg, ccf, cce, ccd, ccc, ccb, cca, cbz, cbr, cbd, cno, cbz; Kerio Personal Firewall 4.0.6-4.0.10, 4.0.16; Microsoft Windows XP Home SP2, XP Professional SP2; Tiny Firewall Pro 6.0.100; Zone Labs ZoneAlarm Pro with Web Filtering 4.5.594</p>	<p>A vulnerability exists due to content filtering bypass issues, which could let a remote malicious user execute arbitrary code on a client system thought to be protected.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Multiple Vendor Content Filtering Bypass</p>	<p>High</p>	<p>Securiteam, November 1, 2004</p>
<p>Multiple Vendors</p> <p>HP HP-UX B.11.23, 11.11, 11.00; Mozilla Network Security Services (NSS) 3.2, 3.2.1, 3.3-3.3.2, 3.4-3.4.2, 3.5, 3.6, 3.6.1, 3.7-3.7.3, 3.7.5, 3.7.7, 3.8, 3.9; Netscape Certificate Server 1.0 P1, 4.2, Directory Server 1.3, P1&P5, 3.12, 4.1, 4.11-4.13, Enterprise Server 2.0 a, 2.0, 2.0.1 C, 3.0 L, 3.0, 3.0.1 B, 3.0.1, 3.1, 3.2, 3.5, 3.6, SP1-SP3, 3.51, 4.0, 4.1, SP3-SP8, Enterprise</p>	<p>A buffer overflow vulnerability exists in the Netscape Network Security Services (NSS) library suite due to insufficient boundary checks, which could let a remote malicious user which may result in remote execute arbitrary code.</p> <p>Mozilla: ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_9_2_RTML/</p> <p>Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57643-1&searchclause=security</p> <p>Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57632-1&searchclause=</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>NSS Buffer Overflow</p>	<p>High</p>	<p>Internet Security Systems Advisory, August 23, 2004</p> <p>Sun(sm) Alert Notification, 57643, September 16, 2004</p> <p>Sun(sm) Alert Notification, 57632, October 25, 2004</p>

Server for NetWare 4/5 3.0.7 a, 4/5 4.1.1, 4/5 5.0, Enterprise Server for Solaris 3.5, 3.6, Netscape Personalization Engine; Sun ONE Application Server 6.0, SP1-SP4, 6.5, SP1 MU1&MU2, 6.5 SP1, 6.5 MU1-MU3, 7.0 UR2 Upgrade Standard, 7.0 UR2 Upgrade Platform, Standard Edition, Platform Edition, 7.0 UR1 Standard Edition, Platform Edition, 7.0 Standard Edition, Platform Edition, Certificate Server 4.1, Directory Server 4.16, SP1, 5.0, SP1&SP2, 5.1 x86 SP3 x86, 5.1, SP1-SP3, 5.2, Web Server 4.1, SP1-SP14, 6.0, SP1-SP7, 6.1				
Netcordia Chesapeake TFTP Server 1.0	Two vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient input validation, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when a malicious user submits an UDP packet that is larger than 514 bytes. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Netcordia Chesapeake TFTP Server Directory Traversal & Remote Denial of Service	Low/Medium (Medium if sensitive information can be obtained)	Secunia Advisory, SA13033, November 1, 2004
openwfe.org Work Flow Engine 1.4-1.4.5	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists in 'login.action' due to insufficient sanitization of input passed to the web client's 'url' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in the 'worklist URL' because arbitrary hosts are accepted, which could let a remote malicious user obtain sensitive information. Update available at: http://sourceforge.net/cvs/?group_id=54621 There is no exploit code required; however, Proofs of Concept exploits have been published.	OpenWFE Remote Cross-Site Scripting & Connection Proxy	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011927, October 26, 2004
Phorum Phorum 5.0.11	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of certain input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists due to insufficient sanitization of unspecified input before being used in a SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Phorum Cross-Site Scripting & SQL Injection	High	Secunia Advisory, SA12980, October 26, 2004
PHP Group PHP 4.0-4.0.7, 4.0.7 RC1-RC3, 4.1.0-4.1.2, 4.2.0-4.2.3, 4.3-4.3.8, 5.0 candidate 1-3, 5.0.0-5.0.2	A vulnerability exists in the 'open_basedir' directory setting due to a failure of the cURL module to properly enforce restrictions, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP cURL Open_Basedir Restriction Bypass	Medium	SecurityTracker Alert ID, 1011984, October 28, 2004
phpCodeGenie phpCodeGenie 1.1, 1.4, 1.21, 3.0 Alpha	A vulnerability exists because php code may be injected through header and footer input, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://phpcodegenie.sourceforge.net/downloads.php There is no exploit code required.	phpCodeGenie Remote Arbitrary Code Execution	High	SecurityTracker Alert ID, 1011911, October 24, 2004
PostNuke Development Team PostNuke 0.75	A vulnerability exists because 'downloads.postnuke.com' was compromised and some files in the PostNuke .750 distribution were modified, which could let a remote malicious user execute arbitrary code. This is due to a vulnerability in the 'pafiledb' download management software <i>Note: The compromise occurred on October 24, 2004 at 23:50 GMT; and the original software was restored on October 26, 2004 at 8:30 GMT.</i> Solution available at: http://securitytracker.com/alerts/2004/Oct/1011938.html There is no exploit code required.	PostNuke Trojan Horse	High	SecurityTracker Alert ID, 1011938, October 26, 2004
Quicksilver Software Master of Orion III	Multiple remote Denial of Service vulnerabilities exist due to a failure to properly handle exceptional conditions.	Quicksilver Master of Orion III Multiple Remote Denials of	Low	Bugtraq, October 27, 2004

1.2.5	No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Service		
Raditha Dissanayake Mega Upload Progress Bar 1.30, 1.35, 1.43, 1.44	A vulnerability exists in 'upload.cgi' due to an unspecified error in the way the file is passed to the PHP handler, which could let a remote malicious user obtain or modify sensitive information. Updates available at: http://sourceforge.net/project/showfiles.php?group_id=87646 We are not aware of any exploits for this vulnerability.	Raditha Dissanayake Mega Upload FileNames	Medium	Secunia Advisory, SA12993, October 27, 2004
RealNetworks RealOne Player 1.0, 2.0, RealPlayer 10.0 BETA, 10.0 v6.0.12.690, 10.0, 10.5 v6.0.12.1053, 10.5 v6.0.12.1040, 10.5 Beta v6.0.12.1016, 10.5	A buffer overflow vulnerability exists in 'DUNZIP32.DLL' due to insufficient boundary checks on filenames contained in skin file archives, which could let a remote malicious user execute arbitrary code. Fixes are available via the 'Check for Update' feature. We are not aware of any exploits for this vulnerability.	RealPlayer Skin File Buffer Overflow	High	eEye Digital Security Advisory, October 26, 2004
Richard Ellerbrock IPplan 2.91, 2.92, 2.99, 3.0 1, 3.0, 3.2	Several input validation vulnerabilities exists due to insufficient validation of numerous variables, which could let a remote malicious user execute arbitrary SQL commands. Updates available at: http://prdownloads.sourceforge.net/iptrack/ipplan-4.00.tar.gz?download There is no exploit code required.	Richard Ellerbrock IPplan Input Validation	High	SecurityTracker Alert ID, 1011919, October 25, 2004
SK Soft SKForum 1.0, 1.1, 1.1.5, 1.2, 1.3, 1.4	A vulnerability exists due to an unspecified error in 'my wiki' and 'wiki.' The impact was not specified. Update available at: http://soft.killingar.net/wiki.view.action?wiki=SKForum We are not aware of any exploits for this vulnerability.	SKForum 'my wiki' & 'wiki'	Not Specified	Secunia Advisory, SA12965, October 25, 2004
Stuart Caie cabextract 0.6, 1.0	A Directory Traversal vulnerability exists in the 'create_output_name()' function in 'cabextract.c' due to insufficient input validation, which could let a remote malicious user create or overwrite files. Update available at: http://www.kyz.uklinux.net/downloads/cabextract-1.1.tar.gz Debian: http://security.debian.org/pool/updates/main/c/cabextract There is no exploit code required.	Stuart Caie cabextract Remote Directory Traversal CVE Name: CAN-2004-0916	Medium	Secunia Advisory, SA12882, October 19, 2004 Debian Security Advisory, DSA 574-1, October 28, 2004
Sun Microsystems, Inc. Java Web Proxy Server 3.6, SP1-SP4	Multiple buffer overflow vulnerabilities exist due to insufficient bounds checks prior to copying user-supplied data into memory buffers, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Updates available at: http://www.sun.com/software/download/products/4096ba15.html We are not aware of any exploits for these vulnerabilities.	Sun Java System Web Proxy Server Multiple Buffer Overflows	Low/High (High if arbitrary code can be executed)	Sun(sm) Alert Notification, 57606, October 29, 2004

Recent Exploit Scripts/Techniques

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

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

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
November 2, 2004	everscan-0.8.2.tgz	N/A	A daemonized network scanner that randomly scans at a very slow pace for machines and stores the data to a database. It comes with a client to query for finds.
November 2, 2004	SecondOrderCodeInjection.pdf	N/A	Whitepaper discussing how injection of data can later be used to carry out an attack at a different point in time.
November 1, 2004	authfail-1.0.0.tgz	N/A	A tool for adding IP addresses to an ACL when entities from those addresses attempt to log into a system, but cause authentication failures in auth.log. It reads data from auth.log in real time and adds the IP into netfilter with a DROP/REJECT policy.
November 1, 2004	mimedefang-2.48.tar.gz	N/A	A flexible MIME email scanner designed to protect Windows clients from viruses that includes the ability to do many other kinds of mail processing, such as replacing parts of messages with URLs. It can alter or delete various parts of a MIME message according to a very flexible configuration file.
November 1, 2004	nixfo-ng-1.5.tar.gz	N/A	A script that scans Linux-based systems and does a complete inventory of anything installed, available, manipulated, or other wise.
October 30, 2004	ability-ftp-exploit.tar.bz2	No	Exploit for the Code-Crafters Ability Server FTP STOR Argument Remote Buffer Overflow vulnerability.
October 30, 2004	mimedefang-2.47.tar.gz	N/A	A flexible MIME email scanner designed to protect Windows clients from viruses that includes the

			ability to do many other kinds of mail processing, such as replacing parts of messages with URLs.
October 29, 2004	hydra-4.4-src.tar.gz	N/A	A high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more. Includes SSL support, parallel scans, and is part of Nessus.
October 28, 2004	bypassArticle.txt	N/A	Presentation: Bypassing client application protection techniques with notepad.
October 28, 2004	moo3boom.zip	No	Proof of Concept for the Quicksilver Master of Orion III Multiple Remote Denial of Service vulnerabilities.
October 28, 2004	wvftpd.c	No	Script that exploits the WvTftp Processing TFTP Options Buffer Overflow vulnerability.
October 27, 2004	ability.c	No	Exploit for the Code-Crafters Ability Server FTP STOR Argument Remote Buffer Overflow vulnerability.
October 27, 2004	aos2bof.zip	No	Script that exploits the Akella Privateer's Bounty: Age of Sail II Remote Nickname Buffer Overflow vulnerability.
October 27, 2004	chmremote.txt	No	Full write up and exploitation walk-thru for the Microsoft Internet Explorer ms-its scheme/CHM remote code execution vulnerability.
October 27, 2004	FakeRedhatPatchAnalysis.txt	N/A	A full analysis of the fake Fedora-Redhat security alert with trojan source code.
October 27, 2004	gd-graphics.c	Yes	Script that exploits the GD Graphics Library Remote Integer Overflow vulnerability.
October 27, 2004	kismet-2004-10-R1.tar.gz	N/A	An 802.11 layer 2 wireless network sniffer that can sniff 802.11b, 802.11a, and 802.11g traffic. It is capable of sniffing using almost any wireless card supported in Linux, which currently divide into cards handled by libpcap and the Linux-Wireless extensions (such as Cisco Aironet), and cards supported by the Wlan-NG project which use the Prism/2 chipset (such as Linksys, Dlink, and Zoom). Besides Linux, Kismet also supports FreeBSD, OpenBSD and Mac OS X systems.
October 27, 2004	libxmlSploit.c	Yes	Proof of Concept exploit for the Libxml2 Multiple Remote Stack Buffer Overflow vulnerabilities.
October 27, 2004	moo3boom.tar	No	Proof of Concept for the Quicksilver Master of Orion III Multiple Remote Denial of Service vulnerabilities.
October 27, 2004	wx-01.tar.gz	N/A	New Macintosh OS-X rootkit that is roughly based off of adore. It hides itself from kextstat, netstat, utmp and wtmp. Further revisions to include a reverse shell triggered by ARP and DNS packets.
October 26, 2004	libxml_exp.c	Yes	Proof of Concept exploit for the Libxml2 Multiple Remote Stack Buffer Overflow vulnerabilities.
October 26, 2004	mailCarrierExploit.txt	No	Script that exploits the Tabs Laboratories MailCarrier Remote SMTP EHLO/HELO Buffer Overflow vulnerability.
October 26, 2004	wvTftpRemoteRootExploit.c	No	Script that exploits the WvTftp Processing TFTP Options Buffer Overflow vulnerability.

[\[back to top\]](#)

Trends

- The RedHat Linux vendor warned in a message on its web site that an e-mail disguised as a Red Hat patch update is a fake designed to trick users into downloading malware. "Red Hat has been made aware that e-mails are circulating that pretend to come from the Red Hat Security Team," Red Hat Inc. said in the message. "These e-mails tell users to download and install malicious updates. These Trojan updates contain malicious code designed to compromise the systems they run on." For more information, see http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1019189,00.html.
- A new caller ID spoofing site has opened that offers subscribers a simple Web interface to a caller I.D. The service is called Camophone and is similar to star38.com, except that anyone can use it (not just government agencies). For more information, see <http://www.securityfocus.com/news/9822>.

[\[back to top\]](#)

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.

Viruses/Trojans

Top Ten Virus Threats

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

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Bagle-AA	Win32 Worm	Stable	April 2004
6	Netsky-B	Win32 Worm	Stable	February 2004
7	Netsky-Q	Win32 Worm	Stable	March 2004
8	Bagle-Z	Win32 Worm	Slight Increase	April 2004
9	Bagle.AT	Win32 Worm	New to Table	October 2004
10	Netsky-C*	Win32 Worm	New to Table	February 2004

* Netsky-C made a large impact when first emerging in February 2004 and has consistently remained stable, just off the Top 10 list. Several anti-virus vendors have recently raised its rating slightly, which has pushed it into the Top 10.

Viruses or Trojans Considered to be a High Level of Threat

- **Bagle.BB**, Bagle AT- A new version of the Bagle mass-mailing worm was discovered Friday, October 29. Bagle.BB harvests addresses from local files and then uses those addresses in the "from" field to send itself. It also opens a backdoor for remote access to the user's computer. Antivirus software makers have also identified other variants of the Bagle virus that are successfully spreading. This virus can also disable the Windows SP2 firewall. ([CNET News](#), October 29, 2004)

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

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

Name	Aliases	Type
Backdoor.Ranky.J		Win32 Worm
Bagle.BB	Bagle.AQ@mm Bagle.AT Bagle.BC I-Worm.Bagle.at W32.Beagle.AT@mm W32.Beagle.AU@mm W32/Bagle-AU W32/Bagle.AP@mm W32/Bagle.bb@mm W32/Bagle.bc W32/Bagle.BC.worm W32/Bagle.bc@MM Win32.Bagle.AQ WORM_BAGLE.AT Win32.Bagle.AP	Win32 Worm
Bagle.BE	W32/Bagle.BE.worm	Win32 Worm
Bagz.g	I-Worm.Bagz.g W32/Bagz.G@mm	Win32 Worm
Famus.C	W32/Famus.C.worm	Win32 Worm
Futro	Backdoor.Delf.mz Backdoor.Futro	Trojan
Ranky.K	Backdoor.Ranky.K Proxy-FBSR TrojanProxy.Win32.Ranky.ax	Trojan
RBOT.VP	IRC/BackDoor.SdBot.69.AQ W32/Spybot.BEX Worm/Rbot.TO WORM_RBOT.VP	Win32 Worm
Singu.B	BackDoor-CGX Backdoor.Singu.B Backdoor.Win32.Singu.t	Trojan
Spydeleter	AdClicker-BH homepage-network Spyware/Spydeleter Trj/Clicker.W	Spyware Downloader
Troj/Bancban-Z		Trojan
Troj/FPatch-A	ELF_FAKEPATCH.A Linux/Fakepatch-A	Trojan
Trojan.Ceegar		Trojan
Trojan.Disabler		Trojan
Trojan.Ducky.C		Trojan
VBS.Yeno.B@mm		Win32 Worm
VBS.Yeno.C@mm		Win32 Worm
W32.Anpes@mm		Win32 Worm
W32.Beagle@mm!cpl		Win32 Worm
W32.Gaobot.BOW		Win32 Worm
W32.Randex.BRD		Win32 Worm
W32/Agobot-NS	Backdoor.Win32.Agobot.gen	Win32 Worm
W32/Agobot-NU		Win32 Worm
W32/Bagle.dldr		Win32 Worm
W32/Bagle-AU	I-Worm.Bagle.at WORM_BAGLE.AT W32/Bagle.bb@MM	Win32 Worm
W32/Bagle-AV	I-Worm.Bagle.au W32/Bagle.bc@MM	Win32 Worm
W32/Bereb.worm!p2p		Win32 Worm
W32/Forbot-BZ	WOOTBOT	Win32 Worm
W32/Leebad-A	Worm.Win32.Leebad.a W32/Sautor.worm TROJ_ADDUSER.F	Win32 Worm

W32/Mydoom.af@MM	Swash.b	Win32 Worm
W32/MyDoom-AG	I-Worm.Mydoom.ab I-Worm.Win32.Swash.31744 I-Worm/Swash.A W32.Mydoom.AG@mm W32/Swash.A.worm Win32.Mydoom.AE Win32/Swash.A@mm Win32/Swash.D@mm Worm/MyDoom.AE WORM_MYDOOM.AG WORM_SWASH.A	Win32 Worm
W32/Myfip.worm.g		Win32 Worm
W32/Rbot-NV	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-NY		Win32 Worm
W32/Rbot-NZ		Win32 Worm
W32/Rbot-OB	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-OP		Win32 Worm
W32/Rbot-OR	WORM_SDBOT.CC	Win32 Worm
W32/Shodi-F	Win32.HLLP.Shodi.d W32/Shodi.worm.f	Win32 Worm
W97M.Inamo		MS Word Macro Virus
Win32.Bagle.AR	Bagle.AU I-Worm.Bagle.au I-Worm/Bagle.AZ W32.Beagle.AU@mm W32.Beagle.AW@mm W32/Bagle-AU W32/Bagle.bd@MM Win32.Bagle.AR Win32:Beagle-AS WORM_BAGLE.AU	Win32 Worm
Win32.Pcclient		Win32 Worm
Win32.Pcclient.D	Backdoor.Formatador Backdoor/Formatador BKDR_PCCLIENT.D	Win32 Worm
Win32.Pcclient.E	Backdoor.Win32.PcClient.f TROJ_TELZ.A W32/Myfip.worm.h Win32/Myfip.H.Worm	Win32 Worm
WORM_BAGLE.AN		Win32 Worm
WORM_BAGZ.E	I-Worm.Bagz.f W32.Bagz.F@mm W32/Bagz-E W32/Bagz.f@MM W32/Bagz.gen@MM	Win32 Worm
Zafi.C	I-Worm.Zafi.c W32./Zafi.C@mm W32.Erkez.C@mm W32/Zafi-C W32/Zafi.C.worm W32/Zafi.c@MM Win32.Zafi.C Win32/Zafi.C.Worm Win32/Zafi.C@mm WORM_ZAFI.C	Win32 Worm

[\[back to top\]](#)