

US-CERT National Cyber Alert System

SB04-301-Summary of Security Items from October 20 through October 26, 2004

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

Bugs, Holes, & Patches

- Windows Operating Systems
 - [Abyss Web Server MS-DOS Device Names Processing](#)
 - [Akella Age of Sail II Buffer Overflow](#)
 - [Altiris Carbon Copy Solution Privilege Escalation](#)
 - [Altiris Deployment Server Client Authentication Hole](#)
 - [Best Software SalesLogix Multiple Vulnerabilities \(Updated\)](#)
 - [Code-Crafters Ability Server Buffer Overflow](#)
 - [DWC_Articles Input Validation](#)
 - [ElektroPost EPiServer Input Validation Errors](#)
 - [FIL_Security Laboratory Twister Anti-Trojan Virus MS DOS Device Names Scan File Failure](#)
 - [H+BEDV AntiVir Fails to Scan Files Named With MS DOS Device Names](#)
 - [Hummingbird Connectivity Vulnerabilities](#)
 - [LANDesk Error Permits Remote Users to Cause a Denial of Service](#)
 - [Mavel ShixxNote 6.net Buffer Overflow in Font Field \(Updated\)](#)
 - [Microsoft Internet Explorer Two Vulnerabilities](#)
 - [Microsoft Outlook May Display Images in Plaintext Only Mode](#)
 - [Microsoft NNTP Remote Code Execution \(Updated\)](#)
 - [Microsoft Windows XP Error in Explorer in Processing WAV Files](#)
 - [Microsoft WebDav XML Message Handler Denial of Service \(Updated\)](#)
 - [Microsoft SMTP Remote Code Execution \(Updated\)](#)
 - [Microsoft Windows Security Update \(Updated\)](#)
 - [Microsoft Windows Shell Remote Code Execution \(Updated\)](#)
 - [Microsoft Compressed \(zipped\) Folders Remote Code Execution \(Updated\)](#)
 - [Mozilla Firefox Browser Denial of Service](#)
 - [Multiple Vendors Tabbed Browsing Vulnerabilities](#)
 - [Multiple Vendors Altnet ADM ActiveX Control Remote Buffer Overflow](#)
 - [Nortel Contivity VPN Client Open Tunnel Certificate Verification Issue](#)
 - [Novell ZENworks for Desktops Privilege Escalation](#)
 - [Proland Protector Plus MS DOs Device Name Scan Failure](#)
 - [Vypress Tonecast Denial of Service](#)
 - [XPA Systems pGina Default Configuration Remote Denial of Service](#)
- UNIX / Linux Operating Systems
 - [Aladdin Enterprises GhostScript Insecure Temporary File Creation \(Updated\)](#)
 - [Apache mod_ssl SSLCipherSuite Access Validation \(Updated\)](#)
 - [Apache mod_include Buffer Overflow](#)
 - [Apple Safari Cross-Domain Dialog Box Spoofing](#)
 - [CVS Undocumented Flag Information Disclosure \(Updated\)](#)
 - [cPanel Backup & FrontPage Management Remote Arbitrary File Modifications \(Updated\)](#)
 - [cPanel Truncated Password Brute Force](#)
 - [dadaIMC HTML Injection](#)
 - [Debian GNU/Linux Telnetd Invalid Memory Handling \(Updated\)](#)
 - [Gaim Buffer Overflows in Processing MSN Protocol \(Updated\)](#)
 - [Gerhard Rieger Socat Remote Format String](#)
 - [GNU GLibC Insecure Temporary File Creation \(Updated\)](#)
 - [Heiko Stamer openSkat Game Unspecified Security Issues](#)
 - [HP ServiceGuard & Cluster Object Manager Remote Root Access](#)
 - [HP-UX 'STMKFONT' External Executables](#)
 - [HP Tru64 X Window System Elevated Privileges](#)
 - [Konqueror Browser Cross-Domain Dialog Box Spoofing](#)
 - [LibTIFF Buffer Overflows \(Updated\)](#)
 - [MPG123 Remote URL Open Buffer Overflow](#)
 - [Multiple Vendors Zlib Compression Library Remote Denial of Service \(Updated\)](#)
 - [Multiple Vendors Gaim Remote Buffer Overflows \(Updated\)](#)
 - [Multiple Vendors CUPS Error Log Password Disclosure \(Updated\)](#)
 - [Multiple Vendor Ecartis Remote Administrator Privileges](#)
 - [Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows](#)
 - [Multiple Vendors LibPNG Graphics Library Image Height Buffer Overflow](#)
 - [Multiple Vendor IMLib/IMLib2 Multiple BMP Image Decoding Buffer Overflows \(Updated\)](#)
 - [Multiple Vendor BMON Arbitrary Code Execution](#)
 - [Multiple Vendor QT Image File Buffer Overflows \(Updated\)](#)
 - [Multiple Vendor Gaim MSNSLP Remote Buffer Overflow](#)
 - [Multiple Vendor gdk-pixbug BMP, ICO, and XPM Image Processing Errors \(Updated\)](#)
 - [Multiple Vendor Linux Kernel IPTables Logging Rules Remote Denial of Service](#)
 - [Multiple Vendor Linux Kernel Race Conditions](#)
 - [Multiple Vendors TNFTPD Multiple Signal Handler Remote Privilege Escalation \(Updated\)](#)
 - [Multiple Vendor LibXpm Image Decoding Multiple Remote Buffer Overflow \(Updated\)](#)
 - [MySQL 'Mysqldhotcopy' Script Elevated Privileges \(Updated\)](#)
 - [Netbilling NBMEMBER Script Information Disclosure](#)
 - [OpenOffice/StarOffice Insecure Temporary File Permissions \(Updated\)](#)
 - [PostgreSQL Insecure Temporary File Creation \(Updated\)](#)
 - [ProFTPD Login Timing Account Disclosure \(Updated\)](#)
 - [Rob Flynn Gaim Remote Denials of Service](#)
 - [Rob Flynn Gaim Multiple Vulnerabilities \(Updated\)](#)
 - [rssh 'log.c' Format String](#)

- o [SCO OpenServer Multiple Vulnerabilities in MMDF \(Updated\)](#)
- o [Speedtouch USB Driver Format String](#)
- o [Splitbrain.org DokuWiki Access Control Enforcement](#)
- o [Squid Remote Denial of Service \(Updated\)](#)
- o [Sun Solaris LDAP RBAC Root Privileges](#)
- o [SuSE Linux IBM S/390 Kernel Root Privileges](#)
- o [LibTIFF OJPEG Buffer Overflow](#)
- o [Twibright Labs Links Malformed Table Remote Denial of Service](#)
- o [University of Kansas Lynx Malformed HTML Remote Denial of Service](#)
- [Multiple Operating Systems](#)
 - o [AOL Web Mail 'msglist.adp' Cross-Site Scripting](#)
 - o [AOL Journals Email Address Disclosure](#)
 - o [Brooky.com CubeCart Input Validation \(Updated\)](#)
 - o [Cisco IOS Telnet Service Remote Denial of Services \(Updated\)](#)
 - o [Google Input Validation](#)
 - o [Gregory DEMAR Coppermine Photo Gallery Voting Restriction Failure](#)
 - o [IBM Lotus Domino Cross-Site Scripting & HTML Injection](#)
 - o [Infopop UBBThreads Input Validation](#)
 - o [MoniWiki 'wiki.php' Cross-Site Scripting](#)
 - o [Netscape/Mozilla SOAPParameter Constructor Integer Overflow Vulnerability \(Updated\)](#)
 - o [Mozilla / Firefox Certificate Store Corruption Vulnerability \(Updated\)](#)
 - o [Mozilla/Firefox/ Thunderbird Multiple Vulnerabilities \(Updated\)](#)
 - o [Mozilla Multiple Remote Vulnerabilities \(Updated\)](#)
 - o [Mozilla Multiple Memory Corruption & Invalid Pointer](#)
 - o [Mozilla / Mozilla Firefox "onunload" SSL Certificate Spoofing \(Updated\)](#)
 - o [Multiple Vendors Browser Cross-Domain Dialog Box Spoofing](#)
 - o [Multiple Vendors Linux Kernel USB Driver Kernel Memory](#)
 - o [Netscape Web Mail 'msglist.adp' Cross-Site Scripting](#)
 - o [Opera TBODY COL SPAN Memory Corruption](#)
 - o [Opera Web Browser Cross-Domain Dialog Box Spoofing](#)
 - o [PBLang Multiple Security Flaws](#)
 - o [Serendipity Input Validation](#)
 - o [Singapore 'thumb.php' Input Validation](#)
 - o [Stuart Caie cabextract Remote Directory Traversal](#)
 - o [Sun Java 2 Micro Edition \(J2ME\) Sandbox Bypass Restrictions](#)
 - o [Symantec Clientless VPN Gateway 4400 Credential Modification](#)
 - o [Symantec Enterprise Firewall/VPN Appliance Multiple Remote Denials of Service & Configuration Modification \(Updated\)](#)
 - o [Tripwire Email Reporting Format String \(Updated\)](#)
 - o [VERITAS NetBackup Input Validation](#)
 - o [MediaWiki 'Title.php' Cross-Site Scripting \(Updated\)](#)
 - o [YPOPs! Buffer Overflows \(Updated\)](#)

[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
Abyss Abyss Web Server X1	An input validation vulnerability exists, which could allow a remote malicious user to crash the target service. It is reported that a remote user can submit an HTTP request for a URL containing a MS-DOS device name (e.g., CON, PRN, AUX) in the 'cgi-bin' directory to cause the web service to crash. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Abyss Web Server MS-DOS Device Names Processing	Low	SecurityTracker Alert ID, 1011812, October 20, 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.	Akella Age of Sail II Buffer Overflow	High	Secunia Advisory ID, SA12905, October 21, 2004

	A Proof of Concept exploit script has been published.			
Altiris Altiris Carbon Copy Solution 6.0.5257	A vulnerability exists which can be exploited by local malicious users to gain escalated privileges. The vulnerability is caused due to the "CCW32.exe" process invoking the help functionality with SYSTEM privileges. Certain prior versions reportedly also ran the Carbon Copy Scheduler with SYSTEM privileges. No workaround or patch available at time of publishing. There is no exploit required.	Altiris Carbon Copy Solution Privilege Escalation	Medium	SecurityFocus, Bugtraq ID 11500, October 22, 2004
Altiris Altiris Deployment Server 5.x, 6.x; 6.1sp1 and prior versions	An authentication vulnerability was reported in the Altiris Deployment Server which could allow a remote malicious user to obtain full control of all target clients. The 'AClient.exe' client process does not authenticate the Deployment Server when connecting. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Altiris Deployment Server Client Authentication Hole	High	SecurityTracker Alert ID, 1011862, October 21, 2004
Best Software SalesLogix 6	Multiple vulnerabilities were reported in which a remote malicious user can gain administrative access on the application. A remote malicious user can inject SQL commands, determine the installation path, determine passwords, and upload arbitrary files. The vendor has issued a fix, available at: http://support.saleslogix.com/ Proof of Concept exploit script has been published.	Best Software SalesLogix Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011769, October 18, 2004 SecurityFocus, October 18, 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. A Proof of Concept exploit script has been published.	Code-Crafters Ability Server Buffer Overflow	High	Secunia Advisory ID, SA12941, October 25, 2004 SecurityFocus, Bugtraq ID 11508, October 22, 2004
Distinct Web Creations Dwc_Articles 1.6 and prior versions	A vulnerability was reported in Dwc_Articles in which a remote malicious user can inject SQL commands. Nearly all of the scripts do not properly validate user-supplied input. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Dwc_Articles Input Validation	Medium	SecurityTracker Alert ID, 1011909, October 23, 2004
ElektroPost Stockholm AB EPiServer	A vulnerability was reported in EPiServer in which a remote malicious user may be able to view files on the target system, obtain sensitive information, and cause Denial of Service conditions. The vendor has reportedly issued a fix for sensitive information issue in version 4.20. There is no solution for the other vulnerabilities at this time. A Proof of Concept exploit has been published.	ElektroPost EPiServer Input Validation Errors	Low/Medium (Medium if sensitive information can be obtained)	SecurityTracker Alert ID, 1011913, October 25, 2004
FIL Security Laboratory Twister Anti-TrojanVirus 5.5	A vulnerability exists that could permit a remote malicious user to create a file that will not be detected by the application. A file or directory name that contains certain character strings related to MS-DOS device names (e.g., COM1, LPT1, AUX, CON, PRN) will not be scanned by the anti-virus system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Twister Anti-Trojan Virus MS DOS Device Names Scan File Failure	High	SecurityTracker Alert ID, 1011843, October 21, 2004
H+BEDV AntiVir DOS 6.28.00.03, AntiVir Windows Server NT/2000/2003 6.28.01.03, AntiVir Windows Workstation 6.28.00.01	A vulnerability exists that could permit a remote malicious user to create a file that will not be detected by the application. A file or directory name that contains certain character strings related to MS-DOS device names (e.g., COM1, LPT1, AUX, CON, PRN) will not be scanned by the anti-virus system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	H+BEDV AntiVir Fails to Scan Files Named With MS DOS Device Names	High	SecurityTracker Alert ID, 1011842, October 21, 2004
Hummingbird Hummingbird Connectivity 7.1 and 9.0	Two vulnerabilities have been reported in which can be exploited to gain escalated privileges or cause a Denial of Service. The Inetd32 administration tool makes it possible for malicious, local users to configure services including changing the executables that are executed, when a connection is received. A boundary error in the FTP service when handling "XCWD" FTP commands can be exploited by malicious users to crash the service by passing an overly long directory name. The vendor has issued patches: http://connectivity.hummingbird.com/support/nc/request.html We are not aware of any exploits for this vulnerability.	Hummingbird Connectivity Vulnerabilities	Medium	NISCC Vulnerability Advisory 841713/Hummingbird, October 26, 2004
LANDesk Software LANDesk 8	A vulnerability exists that could allow a remote malicious user to connect to the remote desktop port (port 3389) on a target system that is being managed by LANDesk to cause the target system to crash and reboot. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	LANDesk Error Permits Remote Users to Cause a Denial of Service	Low	SecurityTracker Alert ID: 1011787, October 19, 2004

Mavel d.o.o. Software Company ShixxNote 6.net	A buffer overflow vulnerability exists that could permit a remote malicious user to execute arbitrary code on the target system. It is reported that a remote user can supply a specially crafted value for the field that specifies the font. No workaround or patch available at time of publishing. Exploit script has been published.	Mavel ShixxNote 6.net Buffer Overflow in Font Field	High	SecurityTracker Alert ID, 1011672, October 14, 2004 PacketStorm, October 23, 2004
Microsoft Internet Explorer 6	Two vulnerabilities exist in Internet Explorer, which can be exploited by malicious users to compromise a user's system, link to local resources, and bypass a security feature in Microsoft Windows XP SP2. The two vulnerabilities in combination with actions in the ActiveX Data Object (ADO) model can write arbitrary files can be exploited to compromise a user's system. Microsoft advises customers who have applied the latest Internet Explorer update, MS04-038, to set the "Drag and Drop or copy and paste files" option in the Internet and Intranet zone to "Disable" or "Prompt." No patch is currently available. A Proof of Concept exploit has been published.	Microsoft Internet Explorer Two Vulnerabilities CVE Names: CAN-2004-0979 CAN-2004-0727	High	Secunia Advisory ID: SA12889, October 20, 2004 US-CERT Vulnerability Note #630720, October 22, 2004 US-CERT Vulnerability Note #207264, October 19, 2004
Microsoft Outlook	A vulnerability was reported in Microsoft Outlook. The e-mail client may display images even when configured to view messages in plain text. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Outlook May Display Images in Plaintext Only Mode	Low	SecurityTracker Alert ID, 1011890 October 22, 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 We are not aware of any exploits for this vulnerability.	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
Microsoft Windows XP Explorer SP1	A vulnerability was reported in Microsoft Windows XP Explorer in the processing of WAV files. A remote malicious user can create a WAV file that, when loaded by the target user, will consume all available CPU resources on the target system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows XP Error in Explorer in Processing WAV Files	Low	SecurityFocus, Bugtraq ID 11503, October 22, 2004
Microsoft Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Internet Information Services 5.0, Internet Information Services 5.1, Internet Information Services 6.0; Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server,	A Denial of Service vulnerability exists that could allow a malicious user to send a specially crafted WebDAV request to a server that is running IIS and WebDAV. A malicious user could cause WebDAV to consume all available memory and CPU time on an affected server. The IIS service would have to be restarted to restore functionality. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-030.msp An exploit script has been published.	Microsoft WebDav XML Message Handler Denial of Service CVE Name: CAN-2004-0718	Low	Microsoft Security Bulletin MS04-030, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 SecurityFocus, October 20, 2004

<p>S8100 Media Servers</p> <p>Microsoft</p> <p>Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange Server 2003;</p> <p>Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server, S8100 Media Servers</p>	<p>A remote code execution vulnerability exists in the Windows Server 2003 SMTP component because of the way that it handles Domain Name System (DNS) lookups. A malicious user could exploit the vulnerability by causing the server to process a particular DNS response that could potentially allow remote code execution. The vulnerability also exists in the Microsoft Exchange Server 2003 Routing Engine component when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4.</p> <p>Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Microsoft SMTP Remote Code Execution</p> <p>CVE Name: CAN-2004-0840</p>	<p>High</p>	<p>Microsoft Security Bulletin MS04-035, October 12, 2004</p> <p>US-CERT Cyber Security Alert SA04-286A, October 12, 2004</p> <p>US-CERT Vulnerability Note VU#394792, October 15, 2004</p> <p>SecurityFocus, October 20, 2004</p>
<p>Microsoft</p> <p>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 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003, Datacenter Edition, Windows Server 2003, Enterprise Edition, Windows Server 2003, Standard Edition, Windows Server 2003, Web Edition, Windows 98, Windows 98 SE, Windows ME</p> <p>Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, 2.0, Avaya S3400 Message Application Server Avaya S8100 Media Servers</p>	<p>Multiple vulnerabilities are corrected with Microsoft Security Update MS04-032. These vulnerabilities include: Window Management Vulnerability, Virtual DOS Machine Vulnerability, Graphics Rendering Engine Vulnerability, Windows Kernel Vulnerability. These vulnerabilities could permit elevation of privilege, remote code execution, and Denial of Service.</p> <p>A vulnerability exists in the Windows SetWindowLong and SetWindowLongPtr API function calls. In some cases this can be exploited to gain execution control.</p> <p>Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-032.mspx</p> <p>Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Advisories are located at the following locations:</p> <p>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()</p> <p>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()</p> <p>Exploit script has been published.</p>	<p>Microsoft Windows Security Update</p> <p>CVE Name: CAN-2004-0207, CAN-2004-0208, CAN-2004-0209, CAN-2004-0211</p>	<p>High</p>	<p>Microsoft Security Bulletin MS04-032, October 12, 2004</p> <p>US-CERT Cyber Security Alert SA04-286A, October 12, 2004</p> <p>US-CERT Vulnerability Notes, VU#910998, VU#218526, VU#806278, October 13, 2004, VU#119262, October 15, 2004</p> <p>SecurityFocus Bugtraq ID: 11369, October 18, 2004</p> <p>SecurityFocus Bugtraq ID: 11365, October 18, 2004</p>
<p>Microsoft</p> <p>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 Professional, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Windows Server 2003 Datacenter Edition, Windows 98, Windows 98 SE, Windows ME</p>	<p>A Shell vulnerability and Program Group vulnerability exists in Microsoft Windows. These vulnerabilities could allow remote code execution.</p> <p>Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx</p> <p>Bulletin updated to reduce the scope of a documented workaround to only support Windows XP, Windows XP Service Pack 1, and Windows Server 2003.</p> <p>We are not aware of any exploits for these vulnerabilities.</p>	<p>Microsoft Windows Shell Remote Code Execution</p> <p>CVE Names: CAN-2004-0214, CAN-2004-0572</p>	<p>High</p>	<p>Microsoft Security Bulletin MS04-037 v1.1, October 25, 2004</p> <p>US-CERT Cyber Security Alert SA04-286A, October 12, 2004</p> <p>US-CERT Vulnerability Note VU#543864, October 15, 2004</p>
<p>Microsoft</p>	<p>A remote code execution vulnerability exists in Compressed (zipped) Folders</p>	<p>Microsoft</p>	<p>High</p>	<p>Microsoft Security</p>

Windows XP Home Edition, XP Professional, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition Avaya DefinityOne Media Servers; IP600 Media Servers; Modular Messaging (MSS) 1.1, 2.0; S3400 Message Application Server; S8100 Media Servers	because of an unchecked buffer in the way that it handles specially crafted compressed files. A malicious user could exploit the vulnerability by constructing a malicious compressed file that could potentially allow remote code execution if a user visited a malicious web site. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-034.mspx We are not aware of any exploits for this vulnerability. Avaya customers are advised to follow Microsoft's guidance for applying patches. Please see the referenced Avaya advisory at the following location for further details: 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.CSSLv11Detail&executeTransaction=avaya.css.UsageUpdate()	Compressed (zipped) Folders Remote Code Execution CVE Name: CAN-2004-0575		Bulletin MS04-034, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 US-CERT Vulnerability Note VU#649374, October 14, 2004 SecurityFocus, Bugtraq ID 11382, October 18, 2004
Mozilla.org Mozilla Firefox	When attempting to render a large binary file as HTML, the browser will consume all available memory on the target system and hang. Files larger than 5 MB will trigger the flaw. A remote user can cause a Denial of Service. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Mozilla Firefox Browser Denial of Service	Low	SecurityTracker Alert ID, 1011917, October 25, 2004
Multiple Browser Vendors Maxthon (MyIE2) 1.1.039 Avant Browser 9.02 build 101 and 10.0 build 029 stilessoft Netcaptr 7.5.2 Flashpeak Slim Browser 4.x	Two vulnerabilities exist which can be exploited by malicious web sites to obtain sensitive information and spoof dialog boxes. Inactive tabs can launch dialog boxes so they appear to be displayed by a web site in another tab and inactive tabs can gain focus from form fields on web sites in another tab. Successful exploitation would normally require that a user is tricked into opening a link from a malicious web site to a trusted web site in a new tab. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Multiple Vendors Tabbed Browsing Vulnerabilities	Medium	Secunia Advisory ID: SA12731, October 20, 2004 Secunia Advisory ID: SA12717, October 20, 2004 Secunia Advisory ID: SA12966, October 25, 2004 Secunia Advisory ID: SA12983, October 26, 2004
Multiple Vendors Altnet ADM; Grokster Grokster 1.3, 1.3.3, 2.6; KaZaA KaZaA Media Desktop 1.3-1.3.2, 1.6.1, 2.0, 2.0.2, 2.6.4	A buffer overflow vulnerability exists in Altnet Download Manager in the 'IsValidFile()' method, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://www.altnet.com/install/upgrade.asp A Proof of Concept exploit has been published.	Altnet ADM ActiveX Control Remote Buffer Overflow	High	SecurityFocus, September 3, 2004 SecurityFocus, October 22, 2004
Nortel Nortel Contivity Multi-OS VPN Client 4.91	A vulnerability exists in Nortel Contivity VPN Client, potentially allowing malicious users to open a VPN tunnel to the client. When the Contivity VPN Client establishes a connection to a gateway, the gateway certificate isn't checked before the user answers a dialog box. While the dialog box is displayed to the user, the VPN tunnel remains open allowing the gateway network access to the client system. There is no solution at this time. Reportedly, this will be fixed in version 5.1. We are not aware of any exploits for this vulnerability.	Nortel Contivity VPN Client Open Tunnel Certificate Verification Issue	Medium	Secunia Advisory ID, SA12881, October 20, 2004
Novell Novell ZENworks for Desktops 4.0.1	A vulnerability has been reported in Novell ZENworks for Desktops, which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to the Remote Management Agent invoking the ZENworks Remote Control Help functionality with SYSTEM privileges. This can be exploited to execute arbitrary programs with escalated privileges. The vulnerability has been fixed in version 4 SP1b/4.0.1 Interim Release 5: http://support.novell.com/servlet/filedownload/sec/pub/zfd401_ir5.exe We are not aware of any exploits for this vulnerability.	Novell ZENworks for Desktops Privilege Escalation	High	Novell Technical Information Documents TID10095153, October 25, 2004 and TID2969662, October 26, 2004
Proland Software Protector Plus	A vulnerability exists that could permit a remote malicious user to create a file that will not be detected by the application. A file or directory name that contains certain character strings related to MS-DOS device names (e.g., COM1, LPT1, AUX, CON, PRN) will not be scanned by the anti-virus system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Proland Protector Plus MS DOS Device Name Scan Failure	High	SecurityTracker Alert ID, 1011844, October 21, 2004
Vypress Vypress Tonecast version 1.3 and prior	A vulnerability exists due to the software not properly processing malformed media streams. A remote malicious user can send specially crafted data to a target system or to all systems on a subnet to cause the application to crash. No workaround or patch available at time of publishing.	Vypress Tonecast Denial of Service	Low	SecurityTracker Alert ID, 1011784, October 19, 2004

	A Proof of Concept exploit has been published.			
XPA Systems pGina 1.7.6	A configuration vulnerability in pGina could permit a remote malicious user to cause Denial of Service conditions. When the administrator does not disable the "Restart" or "Shutdown" options from the login screen, then a remote user connecting via Remote Desktop can cause the system to reboot or shutdown. Solution: The administrator should disable the shutdown and restart options via the pGina configuration utility. A Proof of Concept exploit has been published.	XPA Systems pGina Default Configuration Remote Denial of Service	Low	SecurityTracker Alert ID, 1011896, October 22, 2004

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

UNIX / Linux Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Aladdin Enterprises Ghostscript 4.3, 4.3.2, 5.10 cl, 5.10.10 -1 mdk, 5.10.10 -1, 5.10.10 mdk, 5.10.10, 5.10.12 cl, 5.10.15, 5.10.16, 5.50, 5.50.8 _7, 5.50.8, 6.51, 6.52, 6.53, 7.0 4-7.07	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-200410-18.xml here is no exploit code required.	GhostScript Insecure Temporary File Creation CVE Name: CAN-2004-0967	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory, GLSA 200410-18, October 20, 2004
Apache Software Foundation Apache 2.0.35-2.0.52	A vulnerability exists when the 'SSLCipherSuite' directive is used in a directory or location context to require a restricted set of cipher suites, which could let a remote malicious user bypass security policies and obtain sensitive information. OpenPKG: ftp://ftp.openpkg.org/release/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-21.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ There is no exploit code required.	Apache mod_ssl SSLCipherSuite Access Validation CVE Name: CAN-2004-0885	Medium	OpenPKG Security Advisory, OpenPKG-SA-2004.044, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-21, October 22, 2004 Slackware Security Advisory, SSA:2004-299-01, October 26, 2004
Apache Software Foundation Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.46, 1.3.7 -dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.29, 1.3.31	A buffer overflow vulnerability exists in the 'get_tag()' function, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. Exploit scripts have been published.	Apache mod_include Buffer Overflow CVE Name: CAN-2004-0940	High	SecurityFocus, October 20, 2004
Apple Safari 1.2.3	A cross-domain vulnerability exists when multiple windows are open, which could let a remote malicious user spoof web page functions. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Apple Safari Cross-Domain Dialog Box Spoofing	Medium	Secunia Advisory, SA12892, October 20, 2004
Concurrent Versions Systems (CVS) 1.11	A vulnerability exists in Concurrent Versions System (CVS) in which a malicious user can exploit to determine the existence and permissions of arbitrary files and directories. The problem is caused due to an undocumented switch to the "history" command implemented in "src/history.c". Using the "-X" switch and supplying an arbitrary filename, CVS will try to access the specified file and returns various information depending on whether the file exists and can be accessed. Upgrade to version 1.11.17 or 1.12.9 available at: https://www.cvshome.org/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:14/cvs.patch Fedora Legacy: http://download.fedoralegacy.org/redhat/ Mandrake: http://www.mandrakesecure.net/en/ftp.php A Proof of Concept exploit has been published.	CVS Undocumented Flag Information Disclosure CVE Name: CAN-2004-0778	Low	DEFENSE Security Advisory 08.16.04 FreeBSD Security Advisory, FreeBSD-SA-04:14, September 20, 2004 Fedora Legacy Update Advisory, FLSA:1735, October 7, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004, October 20, 2004
cPanel, Inc. cPanel 9.4.1- RELEASE-64; 9.9.1- RELEASE-3	Several vulnerabilities exist: a vulnerability exists in the backup feature, which could let a remote authenticated malicious user obtain sensitive information; a vulnerability exists when FrontPage extensions are turned on or off, which could let a remote authenticated malicious user change ownership of critical files; and a vulnerability exists in the '_private' directory when FrontPage extensions are turned on or off, which could let a remote authenticated malicious user change permissions on any file on the target system to 0755. The vendor has released fixes dealing with this issue. Users are advised to update to the latest Edge or Current version of cPanel. This update can be	cPanel Backup & FrontPage Management Remote Arbitrary File Modifications	Medium/ High (High if root access can be obtained)	SecurityTracker Alert ID, 1011762, October 18, 2004 SecurityFocus, October 20, 2004

	<p>uploaded from WHM under 'Update to Latest Version' if the update preferences are set to 'Edge' or 'Current'.</p> <p>Proofs of Concept exploits have been published.</p>			
cPanel, Inc. cPanel 9.4.1- STABLE 65	<p>A vulnerability exists in the webmail feature due to insufficient validation of all password characters, which could let a remote malicious user brute force webmail account passwords.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	cPanel Truncated Password Brute Force	Medium	Secunia Advisory, SA12943, October 22, 2004
dadalMC dadaimc 0.95-0.98.2	<p>A vulnerability exists due to insufficient sanitization of user-supplied input before including in dynamically generated web page content, which could let a remote malicious user execute arbitrary HTML code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	dadalMC HTML Injection	High	SecurityFocus, October 18, 2004
Debian telnetd 0.17 -25, 0.17 -18	<p>A vulnerability exists due to a failure to ensure that memory buffers are properly allocated and deallocated, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code.</p> <p>Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/</p> <p>Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet-ssl</p> <p>We are not aware of any exploits for this vulnerability.</p>	Debian GNU/Linux Telnetd Invalid Memory Handling CVE Name: CAN-2004-0911	Low/High (High if arbitrary code can be executed)	Debian Security Advisory, DSA 556-1, October 3, 2004 Debian Security Advisory DSA 569-1, October 18, 2004
Gaim Gentoo	<p>Multiple vulnerabilities were reported in Gaim in the processing of the MSN protocol. A remote user may be able to execute arbitrary code on the target system. Several remotely exploitable buffer overflows were reported in the MSN protocol parsing functions.</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-12.xml</p> <p>SuSE: http://www.suse.de/de/security/2004_25_gaim.html</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Rob Flynn: http://sourceforge.net/project/showfiles.php?group_id=235&package_id=253&release_id=263425</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.1/patches/packages/gaim-0.82-i486-1.tgz</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>We are not aware of any exploits for this vulnerability.</p>	Gaim Buffer Overflows in Processing MSN Protocol CVE Name: CAN-2004-0500	High	SecurityTracker, 1010872, August 5, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:081, August 13, 2004 Slackware Security Advisory, SSA:2004-239-01, August 26, 2004 Fedora Legacy Update Advisory, FLSA:1237, October 16, 2004
Gerhard Rieger socat 1.0 .x, 1.1 .x, 1.2 .x, 1.3 .x, 1.4 .0.2, 1.4 .0.1, 1.4 .0.0	<p>A format string vulnerability exists in the 'void _msg()' function in 'error.c' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.</p> <p>Socat: http://www.dest-unreach.org/socat/download/socat-1.4.0.3.tar.gz</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-26.xml</p> <p>An exploit script has been published.</p>	Gerhard Rieger Socat Remote Format String	High	socat Security Advisory 1, October 22, 2004 Gentoo Linux Security Advisory, GLSA 200410-26, October 25, 2004
GNU 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>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>There is no exploit code required.</p>	GNU Glibc Insecure Temporary File Creation CVE Name: CAN-2004-0968	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory, GLSA 200410-19, October 21, 2004
Heiko Stamer OpenSkat 1.1-1.9	<p>Several security issues related to the non-interactive zero knowledge protocols exist. The impact was not specified.</p> <p>Upgrades available at: http://freshmeat.net/redis/openskat/36295/url_tgz/openskat-2.0.tar.gz</p> <p>We are not aware of any exploits for this vulnerability.</p>	Heiko Stamer openSkat Game Unspecified Security Issues	Not Specified	SecurityTracker Alert ID, 1011805, October 20, 2004
Hewlett Packard Company Cluster Object Manager B.03.00.01, B.03.00.00, B.02.02.02, B.02.02.00,	<p>A vulnerability exists which could let a remote malicious user obtain root privileges.</p> <p>Patches available at: http://itrc.hp.com</p> <p>We are not aware of any exploits for this vulnerability.</p>	HP ServiceGuard & Cluster Object Manager Remote Root Access	High	HP Security Bulletin, HPSBUX01080 , October 22, 2004

B.02.01.02, B.01.04, A.01.03, Serviceguard A.11.16.00, A.11.15.00, A.11.14, A.11.13, Serviceguard for Linux A.11.15.04, A.11.14.04				
Hewlett Packard Company HP-UX B.11.23, B.11.22, B.11.11, B.11.00	A vulnerability exists in 'stmkfont' due to the way paths to external executables are handled, which could let a malicious user execute arbitrary code. Patches available at: http://itrc.hp.com/ There is no exploit code required.	HP-UX 'STMKFONT' External Executables CVE Name: CAN-2004-0965	High	HP Security Bulletin, HPSBUX01088, October 20, 2004
Hewlett Packard Company Tru64 4.0 G PK4, 4.0 F PK8, 5.1 B-2 PK4 (BL25), 4 5.1 B-1 PK3 (BL24), 5.1 A PK6	A file permissions and a buffer overflow vulnerability exists in the X Window System, which could let a malicious user obtain elevated privileges. Patches available at: http://www.itrc.hp.com/service/patch/ We are not aware of any exploits for this vulnerability.	HP Tru64 X Window System Elevated Privileges	Medium	HP Security Bulletin, HPSBTU01084, October 18, 2004
KDE.org Konqueror 3.2.2 -6	A cross-domain dialog vulnerability exists because inactive tabs can launch dialog boxes so they appear to be displayed by a web site in another tab, 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.	Konqueror Browser Cross-Domain Dialog Box Spoofing	Medium	Secunia Advisory, SA12706, October 20, 2004
libtiff.org LibTIFF 3.6.1	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html Proofs of Concept exploits have been published.	LibTIFF Buffer Overflows CVE Name: CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:109 & MDKSA-2004:111, October 20 & 21, 2004 SuSE Security Announcement, SUSE-SA:2004:038, October 22, 2004 RedHat Security Advisory, RHSA-2004:577-16, October 22, 2004
mpg123.de mpg123 pre0.59s, 0.59r	A buffer overflow vulnerability exists in the 'getauthfromURL()' function due to a boundary error, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	MPG123 Remote URL Open Buffer Overflow	High	Securiteam, October 21, 2004
Multiple Vendors FileZilla Server 0.7, 0.7.1; OpenBSD - current, 3.5; OpenPKG Current,	A remote Denial of Service vulnerability during the decompression process due to a failure to handle malformed input. Gentoo: http://security.gentoo.org/glsa/glsa-200408-26.xml FileZilla: http://sourceforge.net/project/showfiles .	Zlib Compression Library Remote Denial of Service CVE Name: CAN-2004-0797	Low	SecurityFocus, August 25, 2004 SUSE Security Announcement, SUSE-SA:2004:029,

<p>2.0, 2.1; zlib 1.2.1</p>	<p>php?group_id=21558</p> <p>OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/017_libz_patch</p> <p>OpenPKG: 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>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>Multiple Vendors</p> <p>Gaim version 0.75 & prior</p>	<p>Multiple buffer overflow vulnerabilities exist due to boundary errors in the YMSG protocol handler, the oscar protocol handler, various utility functions, and the HTTP proxy connection handling, which could let a remote malicious user execute arbitrary code.</p> <p>Upgrade available at: http://prdownloads.sourceforge.net/ultramagnetic/ultramagnetic-0.81.tar.bz2?download</p> <p>Debian: http://security.debian.org/pool/updates/main/g/gaim/</p> <p>Mandrake: http://www.mandrakesecure.net/en/advisories/</p> <p>RedHat: ftp://updates.redhat.com/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/i386/update/</p> <p>Conectiva: ftp://atualizacoes.cbroneectiva.com/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</p> <p>SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/</p> <p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Gaim Remote Buffer Overflows</p> <p>CVE Names: CAN-2004-0005 CAN-2004-0006 CAN-2004-0007 CAN-2004-0008</p>	<p>High</p>	<p>Red Hat Security Advisory, RHSA-2004:032-01, January 26, 2004</p> <p>Slackware Security Advisory, SSA:2004-026-01, January 27, 2004</p> <p>SuSE Security Announcement, SuSE-SA:2004:004, January 29, 2004</p> <p>Mandrake Linux Security Update Advisory, MDKSA-2004:006-1, January 30, 2004</p> <p>Debian Security Advisory, DSA 434-1, February 5, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:813, February 10, 2004</p> <p>SGI Security Advisory, 20040201-01-U, February 11, 2004</p> <p>Fedora Update Notification, FEDORA-2004-070, February 16, 2004</p> <p>US-CERT Vulnerability Notes, VU#197142, VU#779614, VU#444158, VU#871838, VU#527142, VU#297198, VU#371382, VU#503030, VU#190366, VU#226974, VU#655974, VU#404470, May 2004</p> <p>Fedora Legacy Update Advisory, FLSA:1237, October 16, 2004</p>
<p>Multiple Vendors</p> <p>Apple Mac OS X 10.2-10.2.8, 10.3 -</p>	<p>A vulnerability exists in 'error_log' when certain methods of remote printing are carried out by an authenticated malicious user, which could disclose user passwords.</p>	<p>CUPS Error_Log Password Disclosure</p>	<p>Medium</p>	<p>Apple Security Update, APPLE-SA-2004-09-30, October 4, 2004</p>

<p>10.3.5, OS X Server 10.2-10.2.8, 10.3 - 10.3.5; Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4-5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.21</p>	<p>Update available at: http://www.cups.org/software.php</p> <p>Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04829&platform=osx&method=sa/SecUpd2004-09-30Jag.dmg</p> <p>http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04830&platform=osx&method=sa/SecUpd2004-09-30Pan.dmg</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-06.xml</p> <p>Debian: http://security.debian.org/pool/updates/main/c/cupsys/</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-543.html</p> <p>There is no exploit code required.</p>	<p>CVE Name: CAN-2004-0923</p>		<p>Fedora Update Notification, FEDORA-2004-331, October 5, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200410-06, October 9, 2004</p> <p>Debian Security Advisory, DSA 566-1, October 14, 2004</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2004:116, October 21, 2004</p> <p>RedHat Security Advisory, RHSA-2004:543-15, October 22, 2004</p>
<p>Multiple Vendors</p> <p>Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Ecartis Ecartis 0.129 a, 1.0 .0 snapshot 20030417, 20030416, 20030404, 20030318, 20030312, 20030309, 20030303, 20030227, 20021013, 20020514, 20020427, 20020125, 20020121</p>	<p>A vulnerability exists in 'src/modules/lsg2/lsg2-main.c,' which could let a remote malicious user obtain administrator privileges and modify list settings.</p> <p>Debian: http://security.debian.org/pool/updates/main/e/ecartis/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Ecartis Remote Administrator Privileges</p> <p>CVE Name: CAN-2004-0913</p>	<p>High</p>	<p>Debian Security Advisory, DSA 572-1, October 21, 2004</p>
<p>Multiple Vendors</p> <p>Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.20;</p> <p>Gentoo Linux; GNOME GPdf 0.112; KDE KDE 3.2-3.2.3, 3.3, 3.3.1, kpdf 3.2; RedHat Fedora Core2; Ubuntu ubuntu 4.1, ppc, ia64, ia32, Xpdf Xpdf 0.90-0.93; 1.0.1, 1.0 0a, 1.0, 2.0 3, 2.0 1, 2.0, 3.0</p>	<p>Several integer overflow vulnerabilities exist in 'pdftops/Catalog.cc' and 'pdftops/XRef.cc,' which could let a remote malicious user execute arbitrary code.</p> <p>Debian: http://security.debian.org/pool/updates/main/c/cupsys/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-20.xml</p> <p>KDE: ftp://ftp.kde.org/pub/kde/security_patches/post-3.3.1-kdegraphics.diff</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Xpdf PDFTOPS Multiple Integer Overflows</p> <p>CVE Names: CAN-2004-0888 CAN-2004-0889</p>	<p>High</p>	<p>SecurityTracker Alert ID, 1011865, October 21, 2004</p>
<p>Multiple Vendors</p> <p>Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; libpng libpng 1.0, 1.0.5-1.0.17, ibpng3 1.2 .0-1.2.6; SuSE Linux 9.0; Ubuntu ubuntu 4.1 ppc, 4.1 ia64, 4.1 ia32</p>	<p>A buffer overflow vulnerability exists in the processing of images with excessive height, which could let a remote malicious user execute arbitrary code.</p> <p>Debian: http://security.debian.org/pool/updates/main/libp/libpng/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/libp/libpng/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>LibPNG Graphics Library Image Height Buffer Overflow</p> <p>CVE Name: CAN-2004-0955</p>	<p>High</p>	<p>Debian Security Advisories, DSA 570-1 & 571-1, October 20, 2004</p> <p>SuSE Security Announcement, SUSE-SA:2004:037, October 20, 2004</p> <p>Ubuntu Security Notice 1-1, October 22, 2004</p>
<p>Multiple Vendors</p> <p>Enlightenment Imlib2 1.0-1.0.5, 1.1, 1.1.1;</p>	<p>Multiple buffer overflow vulnerabilities exist in the Imlib/Imlib2 libraries when handling malformed bitmap images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.</p>	<p>IMLib/IMLib2 Multiple BMP Image Decoding Buffer</p>	<p>Low/High (High if arbitrary)</p>	<p>SecurityFocus, September 1, 2004</p> <p>Gentoo Linux</p>

<p>ImageMagick ImageMagick 5.4.3, 5.4.4 .5, 5.4.8 .2-1.1.0 , 5.5.3 .2-1.2.0, 5.5.6 .0- 2003040, 5.5.7.6.0.2; Imlib Imlib 1.9-1.9.14</p>	<p>Imlib: http://cvs.sourceforge.net/viewcvs.py/enlightenment/e17/ ImageMagick: http://www.imagemagick.org/www/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200409-12.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-465.html SuSE:ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57648-1&searchclause= http://sunsolve.sun.com/search/document.do?assetkey=1-26-57645-1&searchclause= TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-480.html We are not aware of any exploits for this vulnerability.</p>	<p>Overflows CVE Names: CAN-2004-0817 CAN-2004-0802</p>	<p>code can be executed)</p>	<p>Security Advisory, GLSA 200409-12, September 8, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:089, September 8, 2004 Fedora Update Notifications, FEDORA-2004-300 &301, September 9, 2004 Turbolinux Security Advisory, TLSA-2004-27, September 15, 2004 RedHat Security Advisory, RHSA-2004:465-08, September 15, 2004 Debian Security Advisories, DSA 547-1 & 548-1, September 16, 2004 Conectiva Linux Security Announcement, CLA-2004:870, September 28, 2004 Sun(sm) Alert Notifications, 57645 & 57648, September 20, 2004 Turbolinux Security Announcement, October 5, 2004 RedHat Security Update, RHSA-2004:480-05, October 20, 2004</p>
<p>Multiple Vendors FreeBSD 4.8-4.10, 5.1, 5.2, 5.2.1-RELEASE; Thomas Graf bmon 1.2.1</p>	<p>A vulnerability exists in bmon, which could let a malicious user execute arbitrary code. FreeBSD has updated their port system to remove the setuid bit from the bmon package. Users of affected packages should upgrade to version 1.2.1_2 or greater of the port. A Proof of Concept exploit script has been published.</p>	<p>BMON Arbitrary Code Execution</p>	<p>High</p>	<p>Securiteam October 17, 2004</p>
<p>Multiple Vendors Gentoo Linux 1.4; RedHat Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1, Desktop 3.0, t Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, 2.1 IA64, 2.1, AS 3, AS 2.1 IA64, AS 2.1' Trolltech Qt 3.0, 3.0.5, 3.1, 3.1.1, 3.1.2, 3.2.1, 3.2.3, 3.3 .0, 3.3.1, 3.3.2; Avaya Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0</p>	<p>Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'read_dib()' function when handling 8-bit RLE encoded BMP files, which could let a malicious user execute arbitrary code; and buffer overflow vulnerabilities exist in the in the XPM, GIF, and JPEG image file handlers, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/q/qt-copy/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-20.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kde/qt-3.1.2-i486-4.tgz SuSE: ftp://ftp.suse.com/pub/suse/i386/update Trolltech Upgrade: http://www.trolltech.com/download/index.html TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57637-1&searchclause=security Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html</p>	<p>QT Image File Buffer Overflows CVE Names: CAN-2004-0691 CAN-2004-0692 CAN-2004-0693</p>	<p>High</p>	<p>Secunia Advisory, SA12325, August 10, 2004 Sun Alert ID: 57637, September 3, 2004 Conectiva Linux Security Announcement, CLA-2004:866, September 22, 2004 RedHat Security Advisories, RHSA-2004:478-13 & RHSA-2004:479-05, October 4 & 6, 2004 SUSE Security Announcement, SUSE-SA:2004:035, October 5, 2004 SecurityFocus, October 18, 2004</p>

	<p>http://rhn.redhat.com/errata/RHSA-2004-479.html</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Avaya: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203389&PAGE=avaya.css.CSSLv1Detail&executeTransaction=avaya.css.UsageUpdate()</p> <p>Proof of Concept exploit has been published.</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>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>Multiple Vendors</p> <p>GNU Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; GNOME gdk-pixbug 0.22 & prior; GTK+ 2.0.2, 2.0.6, 2.2.1, 2.2.3, 2.2.4; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64; RedHat Advanced Workstation for the Itanium Processor 2.1, IA64, Desktop 3.0, Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, ES 2.1 IA64, ES 2.1, AS 3, AS 2.1 IA64, AS 2.1, RedHat Fedora Core1&2; SuSE. Linux 8.1, 8.2, 9.0, x86_64, 9.1, Desktop 1.0, Enterprise Server 9, 8</p>	<p>Multiple vulnerabilities exist: a vulnerability exists when decoding BMP images, which could let a remote malicious user cause a Denial of Service; a vulnerability exists when decoding XPM images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability exists when attempting to decode ICO images, which could let a remote malicious user cause a Denial of Service.</p> <p>Debian: http://security.debian.org/pool/updates/main/g/gdk-pixbuf/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>RedHat: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-28.xml</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>gdk-pixbug BMP, ICO, and XPM Image Processing Errors</p> <p>CVE Names: CAN-2004-0753, CAN-2004-0782, CAN-2004-0783, CAN-2004-0788</p>	<p>Low/High (High if arbitrary code can be executed)</p>	<p>SecurityTracker Alert ID, 1011285, September 17, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200409-28, September 21, 2004</p> <p>US-CERT Vulnerability Notes VU#577654, VU#369358, VU#729894, VU#825374, October 1, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:875, October 18, 2004</p>
<p>Multiple Vendors</p> <p>Linux kernel 2.6 - test1-test11, 2.6-l 2.6.8; SuSE Linux 9.1</p>	<p>A remote Denial of Service vulnerability exists in the iptables logging rules due to an integer underflow.</p> <p>Update available at: http://kernel.org/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel IPTables Logging Rules Remote Denial of Service</p> <p>CVE Name: CAN-2004-0816</p>	<p>Low</p>	<p>SuSE Security Announcement, SUSE-SA:2004:037, October 20, 2004</p>
<p>Multiple Vendors</p> <p>Linux kernel 2.2-2.2.25, 2.4.0-test1-test11, 2.4-2.4.27, 2.6-2.6.8</p>	<p>Two vulnerabilities exist: a vulnerability exists in the terminal subsystem due to a race condition, which could let a malicious user cause a Denial of Service or obtain sensitive information; and a vulnerability exists in the PPP dial-up-port due to a race conditions, which could let a malicious user cause a Denial of Service.</p> <p>Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.9.tar.bz2</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel Race Conditions</p> <p>CVE Name: CAN-2004-0814</p>	<p>Low/Medium (Medium if sensitive information can be obtained)</p>	<p>Secunia Advisory, SA12951, October 22, 2004</p>
<p>Multiple Vendors</p> <p>Luke Mewburn lukemftp 1.5, TNFTPD 20031217; NetBSD Current, 1.3-1.3.3, 1.4 x86, 1.4, SPARC, arm32, Alpha, 1.4.1 x86,</p>	<p>Several vulnerabilities exist in the out-of-band signal handling code due to race condition errors, which could let a remote malicious user obtain superuser privileges.</p> <p>Luke Mewburn Upgrade: ftp://ftp.netbsd.org/pub/NetBSD/misc/tnftp/tnftpd-20040810.tar.gz</p> <p>Apple: http://wsidcar.apple.com/cgi-bin/</p> <p>Debian: http://security.debian.org/pool/updates/main/l/lukemftpd/</p>	<p>TNFTPD Multiple Signal Handler Remote Privilege Escalation</p> <p>CVE Name: CAN-2004-0794</p>	<p>High</p>	<p>NetBSD Security Advisory 2004-009, August 17, 2004</p> <p>Apple Security Update, APPLE-SA-2004-09-07, September 7, 2004</p>

<p>1.4.1, SPARC, sh3, arm32, Alpha, 1.4.2 x86, 1.4.2, SPARC, arm32, Alpha, 1.4.3, 1.5 x86, 1.5, sh3, 1.5.1-1.5.3, 1.6, beta, 1.6-1.6.2, 2.0</p>	<p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-19.xml</p> <p>Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57655-1&searchclause=</p> <p>We are not aware of any exploits for this vulnerability.</p>			<p>Debian Security Advisory DSA 551-1, September 21, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200409-19, September 16, 2004</p> <p>Sun(sm) Alert Notification, 57655, October 15, 2004</p>
<p>Multiple Vendors</p> <p>OpenBSD 3.4, 3.5; SuSE Linux 8.1, 8.2, 9.0, x86_64, 9.1, Linux Enterprise Server 9, 8; X.org X11R6 6.7.0, 6.8; XFree86 X11R6 3.3.6, 4.0, 4.0.1, 4.0.2-11, 4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1, Errata, 4.3.0; Avaya Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0</p>	<p>Multiple vulnerabilities exist: a stack overflow vulnerability exists in 'xpmParseColors()' in 'parse.c' when a specially crafted XPMv1 and XPMv2/3 file is submitted, which could let a remote malicious user execute arbitrary code; a stack overflow vulnerability exists in the 'ParseAndPutPixels()' function in '-create.c' when reading pixel values, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists in the colorTable allocation in 'xpmParseColors()' in 'parse.c,' which could let a remote malicious user execute arbitrary code.</p> <p>Debian: http://security.debian.org/pool/updates/main/i/irmlib/</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>OpenBSD: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>X.org: http://x.org/X11R6.8.1/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-34.xml</p> <p>IBM: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html</p> <p>Avaya: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203389&PAGE=avaya.css.CSSLv1Detail&executeTransaction=avaya.css.UsageUpdate()</p> <p>Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57652-1&searchclause=</p> <p>Proofs of Concept exploits have been published.</p>	<p>LibXpm Image Decoding Multiple Remote Buffer Overflow</p> <p>CVE Names: CAN-2004-0687 CAN-2004-0688</p>	<p>High</p>	<p>X.Org Foundation Security Advisory, September 16, 2004</p> <p>US-CERT Vulnerability Notes, VU#537878 & VU#882750, September 30, 2004</p> <p>SecurityFocus, October 4, 2004</p> <p>SecurityFocus, October 18, 2004</p> <p>Sun(sm) Alert Notification, 5765, October 18, 2004</p>
<p>MySQL AB</p> <p>MySQL 3.23.49, 4.0.20</p>	<p>A vulnerability exists in the 'mysqlhotcopy' script due to predictable files names of temporary files, which could let a malicious user obtain elevated privileges.</p> <p>Debian: http://security.debian.org/pool/updates/main/m/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-02.xml</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-569.html</p> <p>There is no exploit code required.</p>	<p>MySQL 'Mysqlhotcopy' Script Elevated Privileges</p> <p>CVE Name: CAN-2004-0457</p>	<p>Medium</p>	<p>Debian Security Advisory, DSA 540-1, August 18, 2004</p> <p>Gentoo Linux Security Advisory GLSA 200409-02, September 1, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:030, September 6, 2004</p> <p>RedHat Security Advisory, ,RHSA-2004:569-16, October 20, 2004</p>
<p>Netbilling, Inc.</p> <p>nbmember.cgi</p>	<p>A vulnerability exists in the 'nbmember.cgi' script, which could let a remote malicious user obtain sensitive information.</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 script has been published.</p>	<p>Netbilling NBMEMBER Script Information Disclosure</p>	<p>Medium</p>	<p>SecurityFocus, October 22, 2004</p>
<p>OpenOffice</p> <p>OpenOffice 1.1.2, Sun StarOffice 7.0</p>	<p>A vulnerability exists in the '/tmp' folder due to insecure permissions, which could let a malicious user obtain sensitive information.</p> <p>Upgrades available at: http://sunsolve.sun.com/search/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-446.html</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-17.xml</p> <p>There is no exploit code required.</p>	<p>OpenOffice/StarOffice Insecure Temporary File Permissions</p> <p>CVE Name: CAN-2004-0752</p>	<p>Medium</p>	<p>Secunia Advisory, SA12302, September 13, 2004</p> <p>RedHat Security Bulletin, RHSA-2004:446-08, September 15, 2004</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2004:103, September 28, 2004</p>

				Gentoo Linux Security Advisory, GLSA 200410-17, October 20, 2004
PostgreSQL PostgreSQL 7.4.5	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-16.xml There is no exploit code required.	PostgreSQL Insecure Temporary File Creation CVE Name: CAN-2004-0977	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory, GLSA 200410-16, October 18, 2004
ProFTPD.net ProFTPD 1.2.8, 1.2.10; possibly other versions	A vulnerability exists due to a time delay difference in the login process for existing and non-existing usernames, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Another Proof of Concept exploit script has been published.	ProFTPD Login Timing Account Disclosure	Medium	LSS Security Team Advisory, October 14, 2004 PacketStorm, October 26, 2004
Rob Flynn Gaim 0.50-0.75, 0.82, 0.82.1, 1.0, 1.0.1	A remote MSN file transfer and a remote MSN SLP Denial of Service vulnerability exists due to a failure to properly handle exceptional conditions. Upgrades available at: http://prdownloads.sourceforge.net/gaim/gaim-1.0.2.tar.gz?download There is no exploit code required.	Gaim Remote Denials of Service	Low	SecurityFocus, October 20, 2004
Rob Flynn Gaim 0.10 x, 0.10.3, 0.50-0.75	Multiple vulnerabilities exist which could let a remote malicious user execute arbitrary code or cause a Denial of Service: a vulnerability exists during the installation of a smiley theme; a heap overflow vulnerability exists when processing data from a groupware server; a buffer overflow vulnerability exists in the URI parsing utility; a buffer overflow vulnerability exists when performing a DNS query to obtain a hostname when signing on to zephyr; a buffer overflow vulnerability exists when processing Rich Text Format (RTF) messages; and a buffer overflow vulnerability exists in the 'content-length' header when an excessive value is submitted. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-27.xml Rob Flynn: http://sourceforge.net/project/showfiles.php?group_id=235&package_id=253&release_id=263425 Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.0/patches/packages/gaim-0.82-i486-1.tgz Fedora Legacy: http://download.fedoralegacy.org/redhat/ Mandrake: http://www.mandrakesecure.net/en/ftp.php We are not aware of any exploits for this vulnerability.	Gaim Multiple Vulnerabilities CVE Names: CAN-2004-0784 , CAN-2004-0754 , CAN-2004-0785	Low/High (High if arbitrary code can be executed)	SecurityFocus, August 26, 2004 Fedora Legacy Update Advisory, FLSA:1237, October 16, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:110, October 21, 2004
rssh rssh 2.2.1 & prior	A vulnerability exists in 'log.c' due to a format string error, which could let a remote malicious user execute arbitrary code. Update available at: http://www.pizzashack.org/rssh/downloads.shtml We are not aware of any exploits for this vulnerability.	rssh 'log.c' Format String	High	Secunia Advisory, SA12954, 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
Speedtouch USB Driver 1.0, 1.1, 1.2, beta1-beta3, 1.3	A format string vulnerability exists because the 'modem_run,' 'pppaa2,' and 'pppaa3' functions make an unsafe 'syslog()' call due to insufficient sanitization, which could let a malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=32758&package_id=28264&release_id=271734 We are not aware of any exploits for this vulnerability.	Speedtouch USB Driver Format String CVE Name: CAN-2004-0834	High	SecurityFocus, October 21, 2004
splitbrain.org DokuWiki 2004-09-30, 2004-09-25, 2004-09-12, 2004-08-22, 2004-08-15a, 2004-08-15, 2004-08-	A vulnerability exists due to improper enforcement of the the access control list, which could let a remote malicious user access some functions without authorization. Affected functions include recent changes, feed, search, and mediaselectiondialog. Updates available at: http://freshmeat.net/redis/dokuwiki/51558/url_tgz/dokuwiki-2004-10-19.tgz	DokuWiki Access Control Enforcement	Medium	SecurityTracker Alert ID, 1011802, October 20, 2004

08, 2004-07-25, 2004-07-21	There is no exploit code required.			
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 We are not aware of any exploits for this vulnerability.	Squid Remote Denial of Service CVE Name: CAN-2004-0918	Low	iDEFENSE Security Advisory, October 11, 2004 Fedora Update Notification, FEDORA-2004-338, October 13, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-15, October 18, 2004 RedHat Security Advisory, RHSA-2004:591-04, October 20, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:112, October 21, 2004
Sun Microsystems, Inc. Solaris 8.0, 8.0_x86, 9.0, 9.0_x86	A vulnerability exists in 'ldap(1)' when used with Role Based Access Control (RBAC), which could let a malicious user execute arbitrary commands with root privileges. Update available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57657-1 We are not aware of any exploits for this vulnerability.	Sun Solaris LDAP RBAC Root Privileges	High	Sun(sm) Alert Notification, 57657, October 18, 2004
SuSE Linux Enterprise Server for S/390, 9.0	A vulnerability exists due to an incorrectly handled privileged instruction which could let a malicious user obtain root user privileges. <i>Note: Vulnerability only affects SuSE Linux Enterprise Server 9 when it is installed on the IBM S/390 platform.</i> Upgrade available at: ftp://ftp.suse.com/pub/suse/ We are not aware of any exploits for this vulnerability.	SuSE Linux IBM S/390 Kernel Root Privileges CVE Name: CAN-2004-0887	High	SuSE Security Announcement, SUSE-SA:2004:037, October 21, 2004
SuSE LibTIFF LibTIFF 3.6.1; SuSE. Linux 8.1, 8.2, 9.0, 9.1Linux Desktop 1.0, Linux Enterprise Server 9, 8	A buffer overflow vulnerability exists in libtiff on SuSE Linux in the OJPEGVSetField () function in 'libtiff/tif_jpeg.c,' which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Upgrades and patches available at: ftp://ftp.suse.com/pub/suse/ We are not aware of any exploits for this vulnerability.	LibTIFF OJPEG Buffer Overflow CVE Name: CAN-2004-0929	Low/High (High if arbitrary code can be executed)	SUSE Security Announcement, SUSE-SA:2004:038, October 22, 2004
Twibright Labs Links 0.91-0.99	A remote Denial of Service vulnerability exists when handling HTML tables of excessive size. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Links Malformed Table Remote Denial of Service	Low	Bugtraq, October 18, 2004
University of Kansas Lynx 2.7, 2.8-2.8.5, 2.8.5 dev2-5, dev8	A remote Denial of Service vulnerability exists when handling malformed HTML tag sequences and formatting. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Lynx Malformed HTML Remote Denial of Service	Low	Bugtraq, October 18, 2004

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

Multiple Operating Systems - Windows / UNIX / Linux / Other				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
America OnLine America Online Webmail	A Cross-Site Scripting vulnerability exists in the 'msglist.adp' script due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	AOL Web Mail 'msglist.adp' Cross-Site Scripting	High	SecurityTracker Alert ID, 1011791, October 20, 2004
America OnLine AOL	An information disclosure vulnerability exists in AOL Journals, which could let a remote malicious user obtain email addresses. No workaround or patch available at time of publishing.	AOL Journals Email Address Disclosure	Medium	SecurityTracker Alert ID, 1011900, October 22, 2004

	A Proof of Concept exploit has been published.			
brooky.com CubeCart 2.0.1	<p>A vulnerability exists due to insufficient sanitization of the 'cat_id' parameter, which could let a remote malicious user obtain sensitive information.</p> <p>The vendor has recommended the following fix: INSERT if (lis_numeric(\$cat_id)) unset(\$cat_id);</p> <p>BEFORE include("header.inc.php");</p> <p>IN index.php</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	CubeCart Input Validation	Medium	<p>Secunia Advisory, SA12764, October 8, 2004</p> <p>SecurityFocus, October 22, 2004</p>
Cisco Systems IOS R12.x, 12.x	<p>A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted TCP connection to a telnet or reverse telnet port.</p> <p>Potential workarounds available at: http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml</p> <p>We are not aware of any exploits for this vulnerability.</p>	Cisco IOS Telnet Service Remote Denial of Service	Low	<p>Cisco Security Advisory, cisco-sa-20040827, August 27, 2004</p> <p>US-CERT Vulnerability Note VU#384230</p> <p>Cisco Security Advisory, 61671 Rev 2.2, October 20, 2004</p>
Google Google	<p>A Cross-Site Scripting vulnerability exists in the 'custom' script due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Vulnerability has appeared in the press and other public media.</p> <p>A Proof of Concept exploit has been published.</p>	Google Input Validation	High	SecurityTracker Alert ID, 1011786, October 19, 2004
Gregory DEMAR Coppermine Photo Gallery 1.0-1.3.2	<p>A vulnerability exists due to a design error that may allow remote malicious users to cast multiple votes for an image.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	Coppermine Photo Gallery Voting Restriction Failure	Medium	SecurityTracker Alert ID, 1011860, October 21, 2004
IBM Lotus Domino 6.0-6.0.3, 6.5.0-6.5.2	<p>Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to an input validation error in the native Lotus Notes HTML encoding for computed values, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists which could let a remote malicious user inject malicious HTML and script code into the application.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	IBM Lotus Domino Cross-Site Scripting & HTML Injection	High	SecurityFocus, October 18, 2004
Infopop UBB.threads 3.4, 3.5	<p>An input validation vulnerability exists in 'dosearch.php' due to insufficient validation of user-supplied input in the 'Name' parameter, which could let a remote malicious user execute arbitrary SQL commands.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	UBBThreads Input Validation	High	Bugtraq, October 21, 2004
moinmoin.wikiwikiweb.de MoniWiki 1.0.8 & prior	<p>A Cross-Site Scripting vulnerability exists in 'wiki.php' due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Update available at: http://kldp.net/project/showfiles.php?group_id=210&release_id=954</p> <p>A Proof of Concept exploit has been published.</p>	MoniWiki 'wiki.php' Cross-Site Scripting	High	Secunia Advisory, SA12975, October 26, 2004
Mozilla.org Mozilla 1.6 & prior; Netscape 7.0, 7.1, and prior	<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>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>	High	<p>iDEFENSE 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,</p>

				CLA-2004:877, October 22, 2004
Mozilla.org Mozilla 1.6; Mozilla 1.7.x; Mozilla Firefox 0.x	<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>Currently, we are not aware of any exploits for this vulnerability.</p>	Mozilla / Firefox Certificate Store Corruption Vulnerability CVE Name: CAN-2004-0758	Low	<p>Secunia Advisory, SA12076, July 16, 2004 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>
Mozilla.org Mandrakesoft Slackware Mozilla 1.7 and prior; Firefox 0.9 and prior; Thunderbird 0.7 and prior	<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>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>We are not aware of any exploits for this vulnerability.</p>	Mozilla/Firefox/ Thunderbird Multiple Vulnerabilities CVE Name: CAN-2004-0757 CAN-2004-0759 CAN-2004-0761 CAN-2004-0765	High	<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 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>
Mozilla.org Mozilla 0.x, 1.0-1.7.x, Firefox 0.x, Thunderbird 0.x; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2	<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>	Mozilla Multiple Remote Vulnerabilities CVE Names: CAN-2004-0902 CAN-2004-0903 CAN-2004-0904 CAN-2004-0905 CAN-2004-0908	Medium/ High (High if arbitrary code can be executed)	<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,</p>

	<p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Proofs of Concept exploits have been published.</p>			<p>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>Mozilla.org</p> <p>Mozilla Browser 1.0, RC1&2, 1.0.1, 1.0.2, 1.1 Beta, 1.1 Alpha, 1.1, 1.2 Beta, 1.2 Alpha, 1.2, 1.2.1, 1.3, 1.3.1, 1.4 b, 1.4 a, 1.4, 1.4.1, 1.4.2, 1.5, 1.6, 1.7 rc3, 1.7-1.7.3, 1.8 Alpha 2</p>	<p>Multiple memory corruption vulnerabilities exist because certain HTML tag sequences and formatting may cause a remote Denial of Service and possibly execution of arbitrary code; and a remote Denial of Service vulnerability exists when an invalid pointer is dereferenced.</p> <p>No workaround or patch available at time of publishing.</p> <p>Proofs of Concept exploits have been published.</p>	<p>Mozilla Multiple Memory Corruption & Invalid Pointer</p>	<p>Low/High</p> <p>(High if arbitrary code can be executed)</p>	<p>Bugtraq, October 18, 2004</p>
<p>Mozilla.org</p> <p>Mozilla Firefox 0.9.2 and Mozilla 1.7.1 on Windows</p> <p>Mozilla Firefox 0.9.2 on Linux</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. 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>A Proof of Concept exploit has been published.</p>	<p>Mozilla / Mozilla Firefox "onunload" SSL Certificate Spoofing</p> <p>CVE Name: CAN-2004-0763</p>	<p>Medium</p>	<p>Cipher.org, July 25, 2004</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>Multiple Vendors</p> <p>Mozilla Browser 1.7.2, 1.7.3, Camino 0.8, Firefox 0.10.1; Netscape Navigator 7.2</p>	<p>Several vulnerabilities exist: a vulnerability exists when multiple tabs are open, which could let a remote malicious user spoof functions on the web site in the active tab; and a vulnerability exists because a web form field in an inactive tab can gain focus, which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>Vulnerability has appeared in the press and other public media.</p> <p>There is no exploit code required; however, Proof of Concept exploit has been published.</p>	<p>Multiple Vendors Browser Cross-Domain Dialog Box Spoofing</p>	<p>Medium</p>	<p>Secunia Advisory, SA12712, October 20, 2004</p>
<p>Multiple Vendors</p> <p>Linux Kernel USB Driver prior to 2.4.27</p>	<p>A vulnerability exists in certain USB drivers because uninitialized structures are used and then 'copy_to_user(...)' kernel calls are made from these structures, which could let a malicious user obtain uninitialized kernel memory contents.</p> <p>Update available at: http://kernel.org/</p> <p>Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200408-24.xml</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel USB Driver Kernel Memory</p> <p>CVE Name: CAN-2004-0685</p>	<p>Medium</p>	<p>US-CERT Vulnerability Note VU#981134, October 25, 2004</p>
<p>Netscape</p> <p>Netscape Web Mail</p>	<p>A Cross-Site Scripting vulnerability exists in the 'msglist.adp' script due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	<p>Netscape Web Mail 'msglist.adp' Cross-Site Scripting</p>	<p>High</p>	<p>SecurityTracker Alert ID, 1011792, October 20, 2004</p>
<p>Opera Software</p> <p>Opera Web Browser 6.0 win32, 6.0 6, 6.0.6win32, 6.0, 6.0.1-6.0.5 win32, 6.0.1-6.0.3 linux, 6.10 linux, 7.0 win32 Beta 1&2, 7.0 -7.0.3 win32, 7.10, 7.11 j, 7.11 b, 7.11, 7.20 Beta 1 build 2981, 7.20-7.23, 7.50-</p>	<p>A memory corruption vulnerability exists in the 'TBODY' tag when an excessive 'COL SPAN' is specified, 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>Proofs of Concept exploits have been published.</p>	<p>Opera TBODY COL SPAN Memory Corruption</p>	<p>Low/High</p> <p>(High if arbitrary code can be executed)</p>	<p>Bugtraq, October 18, 2004</p>

7.54				
Opera Software Opera Web Browser 7.54	A cross-domain vulnerability exists when multiple windows are open, which could let a remote malicious user spoof web page functions. No workaround or patch available at time of publishing. Vulnerability has appeared in the press and other public media. There is no exploit code required; however, a Proof of Concept exploit has been published.	Opera Web Browser Cross-Domain Dialog Box Spoofing	Medium	Secunia Advisory, SA12713, October 20, 2004
PBLang-Team PBLang 4.x	Multiple security vulnerabilities exist, including a cookie management flaw in CheckLoginStatus() in 'functions.php', a flaw in the pm section in 'admin.php' and 'pmpshow.php', and a password changing vulnerability in 'ucp.php'. The impact was not specified. Update available at: https://sourceforge.net/project/showfiles.php?group_id=62953 We are not aware of any exploits for these vulnerabilities.	PBLang Multiple Security Flaws	Not Specified	Secunia Advisory, SA12880, October 19, 2004
S9Y Serendipity 0.3, 0.4, 0.5, -pl, 0.6, rc1&rc2, pl1-pl3, 0.7 - beta1-beta4	An input validation vulnerability exists when processing the requested URI in 'index.php' and the HTTP Referer field in 'comments.php,' which could let a remote malicious user create an HTTP request that will cause arbitrary content to be displayed. Upgrades available at: http://prdownloads.sourceforge.net/php-blog/serendipity-0.7-rc1.tar.gz?download A Proof of Concept exploit has been published.	Serendipity Input Validation	Medium	Secunia Advisory, SA12909, October 21, 2004
Singapore Singapore prior to 0.9.10	A vulnerability exists in 'thumb.php' due to insufficient validation of user-supplied input, which could let a remote malicious user view files that are not image files on the target system (however, the vendor did not confirm the impact.) Update available at: http://singapore.sourceforge.net/?page=download We are not aware of any exploits for this vulnerability.	Singapore 'thumb.php' Input Validation	Not Specified	SecurityTracker Alert ID, 1011804, October 20, 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 There is no exploit code required.	cabextract Remote Directory Traversal	Medium	Secunia Advisory, SA12882, October 19, 2004
Sun Microsystems, Inc. Java 2 Micro Edition (J2ME)	A vulnerability exists in the Connected Limited Device Configuration (CLDC) implementation in the K Virtual Machine (KVM) bytecode verifier, which could let a remote malicious user bypass Java security mechanisms. No workaround or patch available at time of publishing. Exploit information has been published.	Sun Java 2 Micro Edition (J2ME) Sandbox Bypass Restrictions	Medium	Secunia Advisory, SA12945, October 22, 2004
Symantec Clientless VPN Gateway Version 5.0, Model 4000	Various security vulnerabilities exist in the ActiveX file browser and HTML file browser, which could let a remote malicious user obtain unauthorized access to the system or could lead to unpredictable behavior. Hotfix available at: ftp://ftp.symantec.com/public/english_us_canada/products/sym_clientless_vpn/sym_clientless_vpn_5/updates/hf3-readme.txt We are not aware of any exploits for this vulnerability.	Symantec Clientless VPN Gateway 4400 Credential Modification	Medium	US-CERT Vulnerability Note VU#760256, October 20, 2004
Symantec Firewall/VPN Appliance 100, 200, 200R, Gateway Security 320, 360, 360R	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user conducts a fast map UDP port scan against all ports on the WAN interface; a vulnerability exists when a UDP port scan is conducted against the WAN interface from a source port of UDP 53, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because the default read/write community string used by the firewall is public, which could let a malicious user alter the firewall's configuration. The vendor has released a fixed firmware version (1.63) available at: ftp://ftp.symantec.com/public/updates/ There is no exploit code required.	Symantec Enterprise Firewall/VPN Appliance Multiple Remote Denials of Service & Configuration Modification	Low	Rigel Kent Security & Advisory Services Inc. Advisory, RK-001-04, September 22, 20024 US-CERT Vulnerability Notes VU#329230, VU#441078, & VU#173910, October 20, 2004
Tripwire, Inc. Gentoo Mandrake Tripwire 2.2.1, 2.3.0, 2.3.1 - 2, 2.3.1, 2.4.0, 2.4.2, 3.0.1, 3.0, 4.0, 4.0.1, 4.1, 4.2, Tripwire Open Source 2.3.0, 2.3.1	A format string vulnerability exists in 'pipedmailmessage.cpp' when an e-mail report is generated, which could let a malicious user execute arbitrary code. <i>Note: It is reported that this issue only presents itself when the MAILMETHOD is sendmail.</i> Patch available at: http://securityfocus.com/bid/10454/solution/ Gentoo: http://security.gentoo.org/glsa/glsa-200406.02.xml Mandrake: http://www.mandrakesoft.com/security/advisories	Tripwire Email Reporting Format String CVE Name: CAN-2004-0536	High	SecurityFocus, June 5, 2004 Gentoo Linux Security Advisory, GLSA 200406-02, June 4, 2004 J Mandrakelinux Security Update

	<p>Fedora Legacy: http://download.fedoralegacy.org/redhat/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			<p>Advisory, MDKSA-2004:057, June 8, 2004</p> <p>Fedora Legacy Update Advisory, FLSA:1719, October 23, 2004</p>
<p>Veritas Software</p> <p>NetBackup BusinessServer 3.4, 3.4.1, 4.5, NetBackup DataCenter 3.4, 3.4.1, 4.5, NetBackup Enterprise Server 5.1, NetBackup Server 5.0, 5.1</p>	<p>A input validation vulnerability exists in the 'bpjava-susvc' process used for administration, which could let a remote authenticated malicious user execute commands with root privileges.</p> <p>The vendor has described a configuration workaround available at: http://support.veritas.com/docs/271727</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>VERITAS NetBackup Input Validation</p>	<p>High</p>	<p>SecurityTracker Alert ID: 1011863, October</p>
<p>winkled.sourceforge.net</p> <p>MediaWiki prior to 1.3.7</p>	<p>A Cross-Site Scripting vulnerability exists in 'Title.php' due to insufficient filtering of HTML code from user-supplied input in 'DefaultSettings.php' and 'Title.php,' which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Updates available at: http://prdownloads.sourceforge.net/wikipedia/mediawiki-1.3.7.tar.gz?download</p> <p>There is no exploit code required.</p>	<p>MediaWiki 'Title.php' Cross-Site Scripting</p>	<p>Medium/High</p> <p>(High if arbitrary code can be executed)</p>	<p>SecurityFocus, October 20, 2004</p>
<p>yahoopops.sourceforge.net</p> <p>YPOPs! 0.x</p>	<p>Several buffer overflow vulnerabilities exist in the POP3 and SMTP services, which could let a remote malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Another exploit script has been published.</p>	<p>YPOPs! Buffer Overflows</p>	<p>High</p>	<p>Hat-Squad Advisory, September 27, 2004</p> <p>SecurityFocus, October 18, 2004</p>

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
October 26, 2004	85mod_include.c	No	Proof of Concept exploit for the Apache mod_include Buffer Overflow vulnerability.
October 26, 2004	ethereal-0.10.7.tar.gz	N/A	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
October 26, 2004	javascript.txt	N/A	A write-up discussion on how to use Javascript to spoof what page is actually being visited.
October 26, 2004	navRant.txt	NA	Proof of Concept regarding how easy it is to bypass Norton Antivirus.
October 26, 2004	nmap-3.75.tgz	N/A	A utility for port scanning large networks, although it works fine for single hosts.
October 26, 2004	osx86_mmdfdeliver.c	Yes	Script that exploits the SCO OpenServer MMDF vulnerability.
October 26, 2004	proftpdEnum.c	No	Proof of Concept script that exploits the ProFTPD Login Timing Account Disclosure vulnerability.
October 26, 2004	rkdsan.zip	N/A	A scanner designed to detect whether or not an NT based computer is infected with the Hacker Defender root kit.
October 25, 2004	socat_exp.c	Yes	Script that exploits the Socat Remote Format String vulnerability.
October 24, 2004	creating_a_asp_command_shell_using_BACKUP.txt	N/A	This is a text document that describes how MS SQL can be "tricked" into creating a command.asp script under the webroot, even when you do not have access to 'sa' privs (dbo privs are probably still a must, though). The technique described uses the SQL server 'backup' command.
October 24, 2004	ksb26-2.6.9.tar.gz	N/A	KSB26, Kernel Socks Bouncer for 2.6.x, is a Linux 2.6.x-kernel patch that redirects full tcp connections through a socks5 proxy. KSB26 uses a character device to pass socks5 and the target IPs the Linux kernel.
October 24, 2004	lgool.c	N/A	Lgool is a program that will search Google for a given vulnerability.
October 24, 2004	SetWindowLong_Shatter_Attacks.pdf	N/A	This paper gives an example of the variety of shatter attacks which should be corrected by MS04-032 (KB840987). This sort of attack can typically be used for local privilege escalation.
October 24, 2004	uml.c	N/A	Userspace Logger is functioning code based on the example given in the article in Phrack 51 entitled "Shared Library Redirection". The following functions are logged: read()/recv() output and intercepts open(), open64(), close(), socket(), connect(), exit(). This is an effective keystroke logger, among other things, despite that the author says it is only at the Proof-of-Concept phase.
October 23, 2004	101_shixx.cpp	No	Exploit for the Mavel ShixxNote 6.net Buffer Overflow in Font Field vulnerability.
October 23, 2004	amap-4.7.tar.gz	N/A	Application Mapper is a next-generation scanning tool that allows you to identify the applications that are running on a specific port. It does this by connecting to the port(s) and sending trigger packets.
October 23, 2004	Camou121.exe	N/A	Camouflage v1.2.1 is an incredibly weak steganography tool for Windows that uses various image files and doc files as a carrier to hide arbitrary data inside of.
October 23, 2004	CKFP.zip	N/A	This is a Windows program that "unprotects" files which have been hidden using a

			steganography program called Camouflage. If the Camouflage'd file requires a password, the password is reset to nothing.
October 23, 2004	hitb04-shreeraj-shah.pdf	N/A	"Web Services - Attacks and Defense Strategies, Methods and Tools" presentation that discusses how the web service is the new security Lego Land. The main building blocks are UDDI, SOAP and WSDL. This presentation will briefly touch upon each of these aspects.
October 23, 2004	hitb04-sk-chong.pdf	N/A	"Windows Local Kernel Exploitation" presentation that discusses mechanisms to exploit the Windows Kernel for useful local privilege escalation.
October 23, 2004	hitb04-teo-sze-siong.zip	N/A	"Stealth Virus Design Thru Breeding Concept (Non Polymorphic)" presentation that includes Proof of Concept code samples.
October 23, 2004	SetecAstronomy.pl	N/A	This is a Perl script that can search files to identify whether data has been hidden using a weak steganography tool for Windows named Camouflage.
October 22, 2004	ability-2.34-ftp-stor.py	No	Exploit for the Code-Crafters Ability Server FTP STOR Argument Remote Buffer Overflow vulnerability.
October 20, 2004	akellaPrivateersBountyExploit.zip	No	Script that exploits the Akella Privateer's Bounty: Age of Sail II Remote Nickname Buffer Overflow vulnerability.
October 20, 2004	apacheModIncludeLocalBufferOverflowExploit.c	No	Script that exploits the Apache mod_include Buffer Overflow vulnerability.
October 20, 2004	Intro_to_Win32_Exploits.pdf	N/A	An introduction to writing exploits for the Win32 platform. Walks through creation of an exploit for a real vulnerable piece of software, using OllyDbg to help isolate the fault and exploit it.
October 20, 2004	ms04-030_spl.pl	Yes	Perl script that exploits the Microsoft WebDav XML Message Handler Denial of Service vulnerability.
October 20, 2004	noceegar.html	No	Exploit for the Microsoft Internet Explorer HTML Help Control Local Zone Security Restriction Bypass & File Drag and Drop Embedded Code vulnerabilities.
October 20, 2004	windowsEMF_WMF_Exploit.c	Yes	Script that exploits the Microsoft Windows WMF/EMF Remote Buffer Overflow vulnerability.
October 19, 2004	HOD-ms04032-emf-expl2.c	Yes	Exploit that creates crafted metadata files to exploit Microsoft Internet Explorer 6.0.
October 19, 2004	toneboom.zip	No	Script that exploits the Vyprss Tonecast Remote Denial of Service vulnerability.
October 18, 2004	dc_ypop.c	No	Script that exploits the YPOPs! Buffer Overflows vulnerability.
October 18, 2004	salesLogixFileUploadPoC.pl	Yes	Proof of Concept exploit for the Best Software SalesLogix File Upload vulnerability.
October 16, 2004	bmon.sh	Yes	Proof of Concept exploit for theBMON Arbitrary Code Execution vulnerability.

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

Trends

- Results of a survey of 2,000 consumers conducted in August indicated that consumers, increasingly fearful of identity theft, want more security before they'll engage in online banking and other Internet-based services, according to a survey released Tuesday, October 26. Such findings may indicate the marketplace has reached a tipping point in which security is now viewed by users as an imperative rather than impediment to online usage. For more information, see http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1017458,00.html.

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

Viruses/Trojans

Top Ten Virus Threats

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

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	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	MyDoom-O	Win32 Worm	Stable	July 2004
9	Bagle-Z	Win32 Worm	Stable	April 2004
10	MyDoom.M	Win32 Worm	Stable	July 2004

Table Updated October 26, 2004

Viruses or Trojans Considered to be a High Level of Threat

- Opener** - A script-based threat that spies on Mac users has been discovered. The malware disables Mac OS X's built-in firewall, steals personal information and can destroy data. ([CNET News](#), October 25, 2004)
- Famus.B** - After a series of celebrity related Trojans that spread through social engineering techniques the latest one preys on potential victims' curiosity about the ongoing conflict in Iraq. Antivirus companies warned of a new worm on Monday, October 25, that is sent by email and appears to contain photographs of the Iraq war. The Famus.B worm affects Windows systems and tries to trick users into believing its attached file -- called Iraq.scr -- contains pictures from inside Iraq. This virus type was first reported in May 2004. ([ZDNet News](#), October 26, 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.Emcommander		Trojan
Backdoor.Haxdoor.C		Trojan
Backdoor.Roxe.B	Bloodhound.Exploit.13 Exploit.Win32.MS04-028.gen	Trojan
Backdoor.Sdbot.AE	Backdoor.Win32.Wootbot.gen	Win32 Worm
Bagz.d	W32.Bagz.D@mm W32/Bagz.d@MM	Win32 Worm
Bagz.E	W32/Bagz.E.worm	Win32 Worm
Netsky.AH	W32/Netsky.AH.worm	Win32 Worm
SH/Renepo-A	Opener MacOS.Renepo.A SH.Renepo SH.Renepo.A SH.Renepo.B SH/Renepo-A Sh/Renepo.A.Worm Unix/Opener.Worm MacOS.Renepo.B	Macintosh Worm
StartPage-FG	Troj/Dloader-DG Trojan Trojan.Win32.StartPage.jc TROJ_STARTPGE.R	Trojan
Troj/Banker-EK	PWS-Bancban.gen.b	Trojan: Password Stealer
Trojan.Sens		Trojan
W32.Buchon.A@mm	I-Worm.Buchon.b W32.Netsky.AE@mm W32/Baba-A W32/Buchon.gen@MM W32/Buchon@mm Win32.Buchon.B WORM_BUCHON.B	Win32 Worm
W32.Huayu		Win32 Worm
W32.Mydoom.AG@mm		Win32 Worm
W32.Spybot.FCD	Backdoor.Win32.Rbot.gen W32.Spybot.Worm W32/Sdbot.worm.gen.j	Win32 Worm
W32.Watson.A		Win32 Worm
W32/Baba-A	W32/Netsky-AE I-Worm.Baba.b W32/Netsky.ai@MM W32/Buchon@mm	Win32 Worm
W32/Bagz-D	I-Worm.Bagz.d	Win32 Worm
W32/Forbot-BQ	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Forbot-BR		Win32 Worm
W32/Forbot-BU	Backdoor.Win32.Wootbot	Win32 Worm
W32/Forbot-BW	WORM_WOOTBOT.BM	Win32 Worm
W32/Rbot-NG	Win32.Rbot.gen W32/Sdbot.worm.gen.i WORM_RBOT.RW	Win32 Worm
W32/Rbot-NJ	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-NK	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-NS	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-NS	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-NT	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.j WORM_RBOT.RY	Win32 Worm
W32/Rbot-NU	WORM_RBOT.PK W32/Sdbot.worm.gen.w	Win32 Worm
W32/Spybot-DF	Worm.P2P.SpyBot.gen W32/Spybot.worm.gen.a	Win32 Worm
Win32.Gema.D	PWS-Datei Troj/Cryptldr-A TrojanDownloader.Win32.Crypt TROJ_CRYPT.A W32/Crypter.B@dl Win32/Gema.14336.Trojan	Win32 Worm
Win32.Scranor.A	W32.Narcs W32/Scran.worm Win32/Scranor.A.Worm Worm.P2P.Scranor	Win32 Worm
WORM_BAGZ.C		Win32 Worm
WORM_BAGZ.D	I-Worm.Bagz.d W32.Bagz.E@mm	Win32 Worm

	W32/Bagz-D W32/Bagz.D@mm W32/Bagz.e@MM Win32.Bagz.C	
WORM_BUCHON.B	I-Worm.Baba.B I-Worm.Buchon.b I-Worm/Buchon.B Netsky.AG Netsky.AI W32.Netsky.AE@mm W32/Baba-A W32/Buchon.B@mm W32/Buchon.gen@MM W32/Buchon@mm W32/Netsky-AE W32/Netsky.ah@MM W32/Netsky.AI.worm W32/Netsky.ai@MM W32/Netsky.AJ@mm Win32.Buchon.B Win32.Netsky.AG Win32/Buchon.B@mm Win32/Netsky.AG.Worm Win32:Netsky-AF Worm/Buchon.B WORM_NETSKY.AI	Win32 Worm
WORM_TURON.B		Win32 Worm
WORM_VOTE.L		Win32 Worm

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

Last updated