

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends and viruses identified between August 4 and August 17, 2004.

[Bugs, Holes, & Patches](#)

- [Windows Operating Systems](#)
- [UNIX / Linux Operating Systems](#)
- [Multiple Operating Systems](#)

[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. Updates to items appearing in previous bulletins are listed in **bold**. 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.

Windows Operating Systems Only

- [Adobe Acrobat/Acrobat Reader ActiveX Control Buffer Overflow Vulnerability](#)
- [ACME Labs tthttpd Input Validation Error Discloses Files to Remote Users](#)
- [Clearswift MAILsweeper Fails to Detect and Analyze Some Attachment Formats](#)
- [Clearswift MIMESweeper for Web Directory Traversal Vulnerability](#)
- [IceWarp Web Mail Multiple Unspecified Vulnerabilities](#)
- [Keene Digital Media \(KDM\) Server Multiple Vulnerabilities](#)
- [Microsoft Windows Task Scheduler Vulnerability](#)
- [Microsoft POSIX Vulnerability Could Allow Code Execution](#)
- [Microsoft Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting and Spoofing Attacks](#)
- [Microsoft Internet Explorer Address Bar Spoofing Vulnerability](#)
- [NGSEC StackDefender 1.10 Invalid Pointer Dereference Vulnerability](#)
- [Serv-U Local Privilege Escalation Vulnerability](#)
- [SapparoWorks BlackJumboDog Has Buffer Overflow in the FTP Service](#)
- [Sun JRE Win32 Native Assertion Error Lets malicious Applets Deny Service](#)
- [Sygate Secure Enterprise Multiple Vulnerabilities](#)
- [Symantec Clientless VPN Gateway 4400 Series Multiple Vulnerabilities](#)
- [VentaFax Command Execution Lets Local Users Gain Elevated Privileges](#)
- [WIDCOMM Bluetooth Connectivity Software Buffer Overflow Vulnerabilities](#)

UNIX / Linux Operating Systems Only

- [Adobe Acrobat Reader Shell Command Injection and Buffer Overflow Vulnerability](#)
- [Apache Can Be Crashed By PHP Code](#)
- [Benchmark Designs' WHM Autopilot Backdoor Allows Plaintext Credential Leakage](#)
- [CVSTrac "filediff" Arbitrary Command Execution Vulnerability](#)
- [Ethereal: Multiple security problems](#)
- [Gaim Buffer Overflows in Processing MSN Protocol](#)
- [Geeklog Default Installation Lets Remote Users Access the Installation Script](#)
- [Gentoo Tomcat Privilege Escalation Vulnerability](#)
- [gv Local Buffer Overflow](#)
- [HP-UX Process Resource Manager Bug Lets Local Users Corrupt Files](#)
- [HP VirtualVault / Webproxy Multiple Vulnerabilities in Apache](#)
- [KDE Insecure Temporary File Creation Vulnerability](#)
- [Konqueror Frame Injection Vulnerability](#)
- [Linux Kernel sys_chown\(\) Bug May Let Remote NFS Users Modify Group Permissions on Files](#)
- [Linux Kernel 64-bit to 32-bit File Offset Conversion Errors Disclose Kernel Memory to Local Users](#)
- [Paul L Daniels ripMIME Base64 Decoding May Terminate Prematurely When Decoding Virus Attachments](#)
- [Peter F. Brown Simple Form Open Mail Relay Vulnerability](#)
- [phpMyWebhosting SQL Injection Vulnerabilities](#)
- [Redhat GNOME VFS updates address extfs vulnerability](#)
- [Rsync Input Validation Error in sanitize_path\(\) May Let Remote Users Read or Write Arbitrary Files](#)
- [Shorewall Insecure Temporary File Creation Vulnerability](#)
- [SGI IRIX CDE Multiple Vulnerabilities](#)
- [Sourceforge.net Pavuk Digest Authentication Buffer Overflow Vulnerabilities](#)
- [SoX ".WAV" File Processing Buffer Overflow Vulnerabilities](#)
- [SpamAssassin Lets Remote Users Deny of Service By Sending Malformed Messages](#)
- [Team OpenFTPD Format String Flaw Lets Remote Authenticated Users Execute Arbitrary Code](#)
- [xine Buffer Overflow in Processing 'vcd' Identifiers Lets Remote Users Execute Arbitrary Code](#)

Multiple Operating Systems - Windows / UNIX / Linux / Other

- [AOL Instant Messenger aim:goaway URI Handler Buffer Overflow Vulnerability](#)
- [Apache ap_escape_html Remote Denial of Service](#)
- [Apple Mac OS X Security Update Fixes Multiple Vulnerabilities](#)
- [CuteNews "archive" Parameter Cross-Site Scripting Vulnerability](#)
- [CVS Undocumented Flag Information Disclosure Vulnerability](#)
- [eNdonesia 'mod.php' Input Validation Vulnerability in Search 'query' Parameter Permits Cross-Site Scripting Attacks](#)
- [GoScript Input Validation Hole Lets Remote Users Execute Arbitrary Commands](#)
- [IBM Tivoli Access Manager HTTP Response Splitting Vulnerability](#)
- [Juniper Networks NetScreen ScreenOS Can Be Crashed By Remote Users Due to an SSHv1 Implementation Bug](#)
- [Mark Burgess Cfengine RSA Authentication Heap Corruption](#)
- [Matt Johnston Dropbear SSH Server DSS Verification Vulnerability](#)
- [Moodle Input Validation Flaw in 'post.php' in reply Variable Permits Cross-Site Scripting Attacks](#)
- [Mozilla Multiple Vulnerabilities](#)
- [Nokia IPSO Denial of Service Vulnerability](#)
- [Opera Browser Spoofing Vulnerability](#)
- [JetBoxOne CMS Arbitrary File Upload Vulnerability / JetBoxOne Leaves Account Database Unencrypted](#)
- [PHP-Nuke Search Box Cross-Site Scripting Vulnerabilities](#)
- [PluggedOut Blog Input Validation Hole in 'blogid'](#)
- [PHP Development Group Multiple Vulnerabilities in libpng](#)
- [QuiXplorer Input Validation Hole in 'item' Parameter Discloses Files to Remote Users](#)
- [Simon Tatham PuTTY System Compromise Vulnerability](#)
- [Sun Solaris XDMCP Parsing Vulnerability](#)
- [The Webmaster Guide Board Power forum contains cross-site scripting vulnerability](#)
- [Thompson SpeedTouch Home ADSL Modem Predictable TCP ISN Generation](#)
- [Volker Rattel phpBB Fetch All SQL Injection Vulnerability](#)
- [vRating Discloses Sensitive Information and Grants Administrative Access to Remote Users](#)
- [WackoWiki textsearch Cross-Site Scripting Vulnerability](#)
- [Xavier Cirac Shuttle FTP Suite Directory Traversal Vulnerability](#)

Risk is defined as follows:

- **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
Adobe Systems Adobe Acrobat 5.0.5 and prior, possibly 6.0.2	A buffer overflow vulnerability exists in Acrobat/Acrobat Reader due to a boundary error within the "pdf.ocx" ActiveX component supplied with Adobe Acrobat Reader. A remote malicious user can exploit this vulnerability via a malicious website using a specially crafted URL to potentially execute arbitrary code. Successful exploitation allows remote malicious users to utilize the arbitrary word overwrite to redirect the flow of control and eventually take control of the affected system. Code execution will occur under the context of the user that instantiated the vulnerable version of Adobe Acrobat. No solution is available at this time. Vendor asserts this vulnerability is fixed in version 6.0.2. However, proof of concept code exists that causes a Denial of Service.	Adobe Acrobat/Acrobat Reader ActiveX Control Buffer Overflow Vulnerability CVE Name: CAN-2004-0629	High	iDEFENSE Security Advisory 08.13.04
Acme Laboratories tthttpd 2.07 beta 0.4 10dec99	A input validation vulnerability exists in the Windows port of tthttpd. A remote user can view files on the target system that are located outside of the web document directory. tthttpd does not properly validate user-supplied requests. A remote user can submit a request containing directory traversal characters or a direct path to view files on the system. No solution is available at this time. A Proof of Concept exploit has been published.	tthttpd Input Validation Error Discloses Files to Remote Users	Medium	SecurityFocus 101084 August 2004
Clearswift	Several vulnerabilities exist in MAILsweeper in the processing of encoded or compressed files. A remote user may be able to send a MIME attachment that will not be properly	MAILsweeper Fails to Detect	Medium	SecurityFocus SA123

MAILsweeper prior to 4.3.15	<p>scanned by MAILsweeper. MAILsweeper fails to properly detect several common compression formats, including ZIP 6.0, RAR, and HQX. A remote malicious user can create a malicious attachment in certain formats and have the attachment pass through MAILsweeper without detection.</p> <p>A Denial of Service vulnerability also exists due to an error when processing malformed PowerPoint files which may cause the service to enter an endless loop and exhaust all CPU resources.</p> <p>Update to version 4.3.15 available at: http://download.mimesweeper.com/www/Patches/MAILsweeper_Patches_495ReadMe.htm</p> <p>We are not aware of any exploits for this vulnerability.</p>	and Analyze Some Attachment Formats		<p>August 2004</p> <p>Securi 101095: 13, 2004</p> <p>MAILs for SM Release July 28</p>
Clearswift MIMESweeper for Web prior to 5.0.4	<p>An input validation vulnerability exists in MIMESweeper for Web, which can be exploited by a malicious user to retrieve arbitrary files outside the web root via directory traversal attacks using the "..\", "..\\", "..^", and "../" character sequences.</p> <p>Update to version 5.0.4 or later available at: http://download.mimesweeper.com/www/Patches/MSW4WEB504_ReadMe.htm</p> <p>A Proof of Concept exploit has been published.</p>	MIMESweeper for Web Directory Traversal Vulnerability	Medium	MIMES for We 5.0.4 F Notes
IceWarp IceWarp Web Mail prior to 5.2.8	<p>Multiple vulnerabilities exist in IceWarp Web Mail, which could allow a malicious user to conduct cross-site scripting and SQL injection attacks, access sensitive information, and manipulate the file system.</p> <p>Update to version 5.2.8 available at: http://www.icewarp.com/Download/</p> <p>We are not aware of any exploits for this vulnerability.</p>	IceWarp Web Mail Multiple Unspecified Vulnerabilities	High	<p>Secuni SA122 August 2004</p> <p>IceWarp Mail Release Notes, August 2004</p>
Keene Software Keene Digital Media Server 1.0.2	<p>Multiple vulnerabilities exist in Keene Digital Media Server, which can be exploited by a malicious user to retrieve sensitive information such as passwords and perform administrative tasks. 1) Keene Digital Media Server stores passwords in clear text in the file "dmscore.db" in the installation directory. This may disclose sensitive information to malicious local users. 2) An input validation error within the processing of HTTP requests can be exploited to retrieve arbitrary files via directory traversal attacks. It is possible to bypass the user authentication and perform administrative tasks by accessing the script "/dms/adminusers.kspix" directly.</p> <p>No solution is available at this time. The vendor has stated that the vulnerabilities will be fixed in version 1.0.4.</p> <p>A Proof of Concept exploit has been published.</p>	Keene Digital Media (KDM) Server Multiple Vulnerabilities	Medium	<p>Securi 10109: August 2004</p> <p>Secuni SA122 August 2004</p>
Microsoft MS Windows 2000 SP 2, 3, and 4; XP and XP SP1; XP 64-Bit Edition SP 1	<p>A remote code execution vulnerability exists in the Task Scheduler because of an unchecked buffer during application name validation. A malicious user who successfully exploited this vulnerability could take complete control of an affected system.</p> <p>Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-022.msp</p> <p>Exploit script has been published.</p>	Microsoft Windows Task Scheduler Vulnerability	High	<p>Micros Security Bulletin 022, July 2004</p> <p>Package August</p>
Microsoft INTERIX 2.2	<p>This security bulletin was updated to include the INTERIX product. A privilege elevation vulnerability exists in the POSIX operating system component (subsystem) due to an unchecked buffer. This vulnerability could allow remote code execution on an affected system.</p> <p>Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-020.msp</p> <p>Currently, we are not aware of any exploits for this vulnerability.</p>	POSIX Vulnerability Could Allow Code Execution	High	Micros Security MS04-Update August 2004
Microsoft Exchange Server 5.5 SP4	<p>An input validation vulnerability exists in Microsoft Outlook Web Access in which a malicious user could conduct cross-site scripting attacks. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Outlook Web Access software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.</p> <p>Update available at: http://www.microsoft.com/downloads/details.aspx?FamilyId=66E4E033-5A4C-4EEC-84F1-31F0CA878092&displ aylang=en</p> <p>The update does not require a restart, but it will restart Microsoft Internet Information Services (IIS), the Exchange Store, and the Exchange System Attendant Services. Customers that have customized certain ASP pages should check the advisory for some</p>	Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting and Spoofing Attacks	High	<p>Micros Security MS04-August 2004</p> <p>US-CE Vulner. Note VU#94</p>

	important caveats: http://www.microsoft.com/technet/security/bulletin/ms04-026.mspx Currently, we are not aware of any exploits for this vulnerability.			August 2004
Microsoft Microsoft Internet Explorer 5.01, 5.5, 6	A vulnerability exists in Internet Explorer, which potentially can be exploited by a malicious user to conduct phishing attacks against a user. The vulnerability is caused due to Internet Explorer failing to update the address bar after a sequence of actions has been performed on a named window. This can be exploited to display content from a malicious site while displaying the URL of a trusted site in the address bar. Workaround: Disable Active Scripting. Currently known attack vectors do not work on Windows XP systems with SP2 applied. A Proof of Concept exploit has been published.	Internet Explorer Address Bar Spoofing Vulnerability	Medium	Secunia SA123 August 2004
Next Generation Security StackDefender 1.10 and 2.0	Multiple input validation vulnerabilities exist in StackDefender in the processing of certain hooked kernel function parameters which could allow a local or remote malicious user to cause the target system to crash. StackDefender fails to validate the 'ObjectAttributes' parameter supplied to the ZwOpenFile() and ZwCreateFile() kernel API functions. Also, the 'BaseAddress' parameter supplied to the ZwAllocateVirtualMemory() and ZwProtectVirtualMemory() kernel API functions is not properly validated and can be exploited in a similar fashion. Upgrade to StackDefender 2.10 available at: http://ngsec.com/ngproducts/stackdefender/download.php We are not aware of any exploits for this vulnerability.	NGSEC StackDefender 1.10 Invalid Pointer Dereference Vulnerability CVE Names: CAN-2004-0767 CAN-2004-0766	Low	iDEFENSE Security Advisory August
Rhinosoft Serv-U FTP Server 4.x through 5.1.0.0 inclusive	A default login vulnerability exists in Serv-U that could allow a local unprivileged user to execute commands with SYSTEM privileges using a problem with Serv-U administration. The Serv-U FTP server in all its platforms has a local administration account that can be used to configure the server. This account has a default login and password credentials and is only available through the loopback interface. An unprivileged user can connect to the server with the default login information and use the "SITE EXEC" command to execute arbitrary commands. The commands are run with SYSTEM privileges hence turning Serv-U to a conduit through which administrative commands can be run. No solution is available at this time. A Proof of Concept exploit has been published.	Serv-U Local Privilege Escalation Vulnerability	Medium	Secunia August 2004
SapporoWorks BlackJumboDog FTP Server 3.6.1	A buffer overflow vulnerability exists in which a remote malicious user can execute arbitrary code on the target system. A remote user can send a specially crafted FTP command with a long parameter string to trigger the flaw. The USER, PASS, RETR, CWD, XMKD, XRMD, and other commands are affected. The software reportedly copies the user-supplied parameter string to a 256 byte buffer. Update to version 3.6.2, available at: http://homepage2.nifty.com/spw/software/bjd/ A Proof of Concept exploit has been published.	BlackJumboDog Has Buffer Overflow in the FTP Service	High	US-CERT VU#71 August Secunia August
Sun Microsystems Java Runtime Environment (JRE)	A Denial of Service vulnerability exists in Sun's Java Runtime Environment. A remote malicious user can create a Java applet that alerts using a native win32 assertion that will, when loaded by the target user, cause the target user's system to crash. No solution is available at this time. A Proof of Concept exploit has been published.	Sun JRE Win32 Native Assertion Error Lets malicious Applets Deny Service	Low	Secunia 10108 August
Sygate Sygate Secure Enterprise prior to 3.5MR3 and Sygate Enforcer 4.0 and later	Multiple vulnerabilities exist in Sygate Secure Enterprise (SSE) in the processing of client logging messages which could allow a remote malicious user to cause a Denial of Service or bypass security restrictions. A remote user can cause the service to consume all available resources on the target system by continually replaying HTTP messages and discovery datagrams (UDP). The system does not provide replay protection for messages sent from Sygate Security Agent clients. An optional component, Sygate Enforcer, does not correctly filter broadcast traffic sent prior to authentication, allowing malicious users to bypass the authentication. Update to SSE version 3.5MR3 and a Sygate Enforcer version later than 4.0 available at: http://www.sygate.com/products/sygate-secure-enterprise.htm We are not aware of any exploits for this vulnerability.	Sygate Secure Enterprise Multiple Vulnerabilities CVE Name: CAN-2004-0163	Low	Secunia 10109 August 2004 Corsair Security Advisory c031123, Aug 2004
Symantec Symantec Clientless VPN Gateway 4400 Series	Multiple vulnerabilities exist in Symantec Clientless VPN Gateway 4400 Series, where some have an unknown impact and others can be exploited to conduct cross-site scripting attacks or manipulate users' signon information. Various unspecified vulnerabilities affect the ActiveX and HTML file browsers; input validation errors within the end user UI can be exploited to conduct cross-site scripting attacks; an error within the end user UI can be exploited by a malicious user to manipulate other users' signon information (including username and password).	Symantec Clientless VPN Gateway 4400 Series Multiple Vulnerabilities	High	Symantec Hotfix: 200408 August

	<p>A hotfix is available at: ftp://ftp.symantec.com/public/english_us_canada/products/sym_clientless_vpn/sym_clientless_vpn_5/updates/SCVG5-20040806-00.tgz</p> <p>We are not aware of any exploits for this vulnerability.</p>			
<p>Venta Association</p> <p>VentaFax 5.4</p>	<p>A vulnerability exists in VentaFax that could allow a local malicious user to obtain elevated privileges. A local malicious user can access the application via the system tray and can execute commands with Local System privileges.</p> <p>No solution is available at this time.</p> <p>A Proof of Concept exploit has been published.</p>	<p>VentaFax Command Execution Lets Local Users Gain Elevated Privileges</p>	<p>Medium</p>	<p>Securi 10109 August</p>
<p>WIDCOMM</p> <p>WIDCOMM Bluetooth Connectivity Software versions prior to 3.0 on the BTW and BT-CE/PPC platforms</p> <p>BTStackServer 1.3.2.7 and 1.4.2.10 on both Windows XP and Windows 98</p> <p>HP IPAQ 5450 running WinCE 3.0 with Bluetooth software version 1.4.1.03.</p>	<p>Multiple buffer overflow vulnerabilities exist in WIDCOMM Bluetooth Connectivity Software which a malicious user can use to execute arbitrary code. The vulnerabilities are caused due to boundary errors when handling various malformed service requests. These can be exploited by sending specially crafted service requests through a wireless Bluetooth connection to a vulnerable system.</p> <p>No solution is available at this time. The vendor reports that issues will be fixed in version 3.</p> <p>A Proof of Concept exploit has been written.</p>	<p>WIDCOMM Bluetooth Connectivity Software Buffer Overflow Vulnerabilities</p> <p>CVE Name: CAN-2004-0775</p>	<p>High</p>	<p>Securi SA122 August 2004</p> <p>Pentes Securi Adviso 2004-C August 2004</p>

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

UNIX / Linux Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
<p>Adobe Systems</p> <p>Adobe Acrobat Reader 5.05 and 5.06</p>	<p>An input validation and boundary error vulnerability exists in the uudecoding feature of Adobe Acrobat Reader, which can be exploited by a malicious user to compromise a user's system. An input validation error injection of arbitrary shell commands. The boundary vulnerability can be exploited to cause a buffer overflow via a malicious PDF document with an overly long filename. Successful exploitation may allow execution of arbitrary code, but requires that a user is tricked into opening a malicious document.</p> <p>Update to version 5.09 for UNIX available at: http://www.adobe.com/products/acrobat/readstep2.html</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Adobe Acrobat Reader Shell Command Injection and Buffer Overflow Vulnerability</p> <p>CVE Names: CAN-2004-0630 CAN-2004-0631</p>	<p>High</p>	<p>Secunia, SA12285, August 13, 2004</p> <p>iDEFENSE Advisories 08.12.04</p>
<p>Apache Software Foundation</p> <p>Apache 2.0.49 (Win32) with PHP 5.0.0 RC2</p>	<p>A Denial of Service vulnerability exists in the Apache web server when running with PHP due to a flaw when invoking certain functions such as fopen and fsockopen in an endless loop.</p> <p>Hewlett-Packard: Install updated version of Apache from Software Depot. http://software.hp.com</p> <p>Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000857</p> <p>A Proof of Concept exploit has been published.</p>	<p>Apache Can Be Crashed By PHP Code</p>	<p>Low</p>	<p>SecurityTracker, 1010674, July 9, 2004</p> <p>US-CERT Cyber Security Bulletin SB04-203</p> <p>HP SSR4777 rev. 0 HP-UX Apache, PHP, August 2, 2004</p> <p>Secunia, SA12243, August 9, 2004</p>

Benchmark Design WHM Autopilot 2.4.5 and prior	A login vulnerability exists due to a bug in client login code and the built-in login backdoor. It is possible to generate the hash required to get a user's username and plain-text password. No solution is available at this time. We are not aware of any exploits for this vulnerability.	Benchmark Designs' WHM Autopilot Backdoor Allows Plaintext Credential Leakage	Medium	SecuriTeam, August 3, 2004
cvstrac.org CVSTrac 1.1.3	An input validation vulnerability exists in CVSTrac due to insufficient sanitization of input passed to 'filediff,' which could allow a malicious user to execute arbitrary code. Fix available in the CVS repository at: http://www.cvstrac.org/cvstrac/wiki?p=DownloadCvstrac A Proof of Concept exploit has been published.	CVSTrac "filediff" Arbitrary Command Execution Vulnerability	High	Bugtraq, August 5, 2004
Ethereal Ethereal 0.x	Multiple Denial of Service and buffer overflow vulnerabilities exist due to errors in the iSNS, SNMP, and SMB dissectors which may allow a malicious user to run arbitrary code or crash the program. Updates available at: http://www.ethereal.com/download.html or disable the affected protocol dissectors. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Debian: http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00129.html <i>Exploit script has been published.</i>	Ethereal: Multiple security problems CVE Names: CAN-2004-0633 CAN-2004-0634 CAN-2004-0635	High	Ethereal Advisory, enpa-sa-00015, July 6, 2004 Gentoo Linux Security Advisory, GLSA 200407-08 / Ethereal, July 9, 2004 Secunia Advisory, 12034 & 12035, July 12, 2004 <i>SecurityFocus, August 5, 2004</i>
Gaim Gentoo	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. Gentoo: http://security.gentoo.org/glsa/glsa-200408-12.xml SuSE: http://www.suse.de/de/security/2004_25_gaim.html We are not aware of any exploits for this vulnerability.	Gaim Buffer Overflows in Processing MSN Protocol CVE Name: CAN-2004-0500	High	SecurityTracker, 1010872, August 5, 2004
Geeklog.net Geeklog 1.39	A configuration vulnerability exists in Geeklog. The installation software leaves the 'install' file in the 'admin' directory, which is accessible to remote users. A remote malicious user can invoke the installation script with specially crafted URLs. No solution is available at this time. We are not aware of any exploits for this vulnerability.	Geeklog Default Installation Lets Remote Users Access the Installation Script	Low	SecurityTracker 1010948, August 13, 2004
Gentoo Linux 1.x versions prior to "www-servers/tomcat-5.0.27-r3"	A privilege escalation vulnerability exists in the tomcat package for Gentoo, which can be exploited by a local malicious user to escalate their privileges. tomcat initialization scripts are owned by the "tomcat" user and group, but are run with "root" privileges during system startup. This can be exploited by users in the "tomcat" group to execute commands as root. Update to "www-servers/tomcat-5.0.27-r3" or later. http://security.gentoo.org/glsa/glsa-200408-15.xml We are not aware of any exploits for this vulnerability.	Gentoo Tomcat Privilege Escalation Vulnerability	Medium	Gentoo Security Advisory, GLSA 200408-15 / tomcat, August 15, 2004
gv Postscript and PDF viewer 3.5.8 and prior Gentoo	A buffer overflow vulnerability exists in gv that could allow a local malicious user to execute arbitrary code. To exploit this vulnerability, a malicious user would have to trick a user into viewing a malformed PDF or PostScript file from the command. Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200408-10.xml A Proof of Concept exploit script has been published.	gv Local Buffer Overflow	High	SecuriTeam, August 4, 2004
Hewlett-Packard	A vulnerability was reported in the HP-UX Process Resource Manager	HP-UX Process	Medium	HP SSRT4785

<p>HP-UX Process Resource Manager C.02.01[.01] and prior</p> <p>HP-UX Workload Manager</p>	<p>that could allow non-root local malicious users to corrupt data files on a system that has the Process Resource Manager installed. Workload Manager (version A.02.01 and prior) includes the Process Resource Manager and, therefore, is also affected.</p> <p>For Proc-Resrc-Mgr.PRM-RUN (PRM-Sw-Lib.PRM-LIB), install revision C.02.02 or subsequent. For WLM-Monitor (Workload-Mgr), install revision A.02.02 or subsequent. Update information and patch matrix is available at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBUX01065</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Resource Manager Bug Lets Local Users Corrupt Files</p>		<p>rev. 0 HP-UX Process Resource Manager (PRM) potential data corruption, August 5, 2004</p> <p>SecurityTracker: 1010914, August 10, 2004</p>
<p>Hewlett-Packard</p> <p>HP-UX release B.11.04 with VirtualVault A.04.50 - A.04.70 or Webproxy A.02.00 - A.02.10</p>	<p>Multiple vulnerabilities exist in Apache affecting HP VirtualVault and HP Webproxy, which can be exploited by a malicious user to cause a DoS (Denial of Service), bypass security restrictions, or compromise a vulnerable system.</p> <p>Install patches available at: http://itrc.hp.com</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>HP VirtualVault / Webproxy Multiple Vulnerabilities in Apache</p>	<p>High</p>	<p>Secunia, SA12246, August 10, 2004</p> <p>SSRT4788 rev. 0 HP-UX Apache, August 8, 2004</p> <p>SSRT4789 rev. 0 HP-UX Apache, August 8, 2004</p>
<p>KDE 3.2.3 and prior</p>	<p>Two vulnerabilities exist in KDE which a local malicious user can exploit to gain escalated privileges and unauthorized access to files on the system. 1) Certain directories and files are created insecurely when a user runs a KDE application outside the KDE environment or as another user. This can be exploited via symlink attacks to overwrite or truncate arbitrary files or prevent KDE applications from accessing certain directories. 2) The DCOPServer creates temporary files, which are used for authentication related purposes, insecurely. This can be exploited to potentially gain the privileges of any user running a KDE application.</p> <p>Apply patches available at: ftp://ftp.kde.org/pub/kde/security_patches/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-13.xml</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>KDE Insecure Temporary File Creation Vulnerability</p> <p>CVE Name: CAN-2004-0690</p>	<p>Medium</p>	<p>KDE Security Advisories 20040811-1 and 20040811-2, August 11, 2004</p>
<p>KDE 3.2.3 and prior</p>	<p>A frame injection vulnerability exists in the Konqueror web browser that allows websites to load web pages into a frame of any other frame-based web page that the user may have open. A malicious website could abuse Konqueror to insert its own frames into the page of an otherwise trusted website. As a result the user may unknowingly send confidential information intended for the trusted website to the malicious website.</p> <p>Source code patches have been made available which fix these vulnerabilities. Refer to advisory: http://www.kde.org/info/security/advisory-20040811-3.txt</p> <p>A Proof of Concept exploit has been published.</p>	<p>Konqueror Frame Injection Vulnerability</p> <p>CVE Name: CAN-2004-0721</p>	<p>Low</p>	<p>KDE Security Advisory 20040811-3, August 11, 2004</p>
<p>Linux 2.4.27</p>	<p>A permissions vulnerability exists in the sys_chown() module of the Linux kernel. A remote authenticated user can modify the group permissions of files on the target system. A remote malicious user can modify the group ID of arbitrary files on the system due to a missing check for fsuid in the sys_chown() function. An NFS client may be able to make unauthorized changes to the group ownership of files on a remote system.</p> <p>Upgrade to Linux 2.4.27 RC5.</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel sys_chown() Bug May Let Remote NFS Users Modify Group Permissions on Files</p> <p>CVE Name: CAN-2004-0497</p>	<p>Medium</p>	<p>SecurityTracker, 1010859, August 4, 2004</p>
<p>Linux Fedora RedHat SuSE</p> <p>Linux kernel 2.4 through 2.4.26, 2.6 through 2.6.7</p>	<p>A vulnerability exists in the Linux kernel in the processing of 64-bit file offset pointers thus allowing a local malicious user to view kernel memory. The kernel's file handling API does not properly convert 64-bit file offsets to 32-bit file offsets. In addition, the kernel provides insecure access to the file offset member variable. As a result, a local user can gain read access to large portions of kernel memory.</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>RedHat: http://rhn.redhat.com/</p>	<p>Linux Kernel 64-bit to 32-bit File Offset Conversion Errors Disclose Kernel Memory to Local Users</p> <p>CVE Name: CAN-2004-0415</p>	<p>High</p>	<p>ISEC Security Research, August 4, 2004</p>

	<p>SuSE: http://www.suse.de/de/security/2004_24_kernel.html</p> <p>A Proof of Concept exploit has been published.</p>			
<p>Paul L Daniels</p> <p>ripMIME 1.3.2.2 and prior</p>	<p>An input validation vulnerability exists in ripMIME, which may allow a virus to avoid detection and compromise the system. Certain virus attachments may not be properly decoded. Some viruses use encoded attachments that may contain blank lines or other invalid characters to cause the Base64 decoding process to terminate prematurely. As a result, an anti-virus system using this decoding method may fail to detect a virus.</p> <p>Update to version 1.3.2.3, available at: http://www.pldaniels.com/ripmime/downloads.php</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>ripMIME Base64 Decoding May Terminate Prematurely When Decoding Virus Attachments</p>	<p>Medium</p>	<p>SecurityTracker, 1010858, August 4, 2004</p>
<p>Peter F. Brown</p> <p>Simple Form prior to 2.2</p>	<p>An input validation vulnerability exists in Simple Form, which can be exploited by a malicious user to use it as an open mail relay. Input passed to the parameters "admin_email_to" and "admin_email_from" isn't properly verified before being used in mails.</p> <p>Update to version 2.2 available at: http://worldcommunity.com/opensource/utilities/simple_form.html</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Simple Form Open Mail Relay Vulnerability</p>	<p>Low</p>	<p>Secunia, SA12297, August 16, 2004</p>
<p>phpMyWebhosting version 0.3.4</p>	<p>Multiple input validation vulnerabilities exist in phpMyWebhosting that allow malicious users to gain elevated privileges as well as enter to the product's management system without knowing the administrative password. phpMyWebhosting does not verify incoming user input for arbitrary SQL statements. If magic_quotes_gpc is disabled in PHP settings, a remote malicious user can cause SQL injection vulnerability in phpMyWebhosting.</p> <p>No solution is available at this time.</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>phpMyWebhosting SQL Injection Vulnerabilities</p>	<p>High</p>	<p>SecuriTeam, August 16, 2004</p>
<p>Redhat</p> <p>GNOME VFS</p> <p>Red Hat Enterprise Linux AS (Advanced Server) version 2.1 - i386, ia64; Red Hat Linux Advanced Workstation 2.1 - ia64; Red Hat Enterprise Linux ES version 2.1 - i386; Red Hat Enterprise Linux WS version 2.1 - i386; Red Hat Enterprise Linux AS version 3 - i386, ia64, ppc, s390, s390x, x86_64 Red Hat Desktop version 3 - i386, x86_64; Red Hat Enterprise Linux ES version 3 - i386, ia64, x86_64; Red Hat Enterprise Linux WS version 3 - i386, ia64, x86_64</p>	<p>Multiple vulnerabilities exist in several of the GNOME VFS extfs backend scripts. Red Hat Enterprise Linux ships with vulnerable scripts, but they are not used by default. A malicious user who is able to influence a user to open a specially-crafted URI using gnome-vfs could perform actions as that user. Users of Red Hat Enterprise Linux should upgrade to these updated packages, which remove these unused scripts.</p> <p>Before applying this update, make sure that all previously-released errata relevant to your system have been applied. Use Red Hat Network to download and update your packages. To launch the Red Hat Update Agent, use the following command: up2date</p> <p>For information on how to install packages manually, refer to the following Web page for the System Administration or Customization guide specific to your system: http://www.redhat.com/docs/manuals/enterprise/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>GNOME VFS updates address extfs vulnerability</p> <p>CVE Name: CAN-2004-0494</p>	<p>High</p>	<p>Red Hat Security Advisory ID: RHSA-2004:373-01, August 4, 2004</p>
<p>Shorewall 1.4.x, 2.0.x</p>	<p>A privilege escalation vulnerability is caused due to the "shorewall" script creating temporary files insecurely, which can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user invoking the script (usually root).</p> <p>Update available at: http://shorewall.net/download.htm</p> <p>Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:080</p> <p>Currently, we are not aware of any exploits for this vulnerability.</p>	<p>Shorewall Insecure Temporary File Creation Vulnerability</p> <p>CVE Name: CAN-2004-0647</p>	<p>Medium</p>	<p>Shorewall Security Vulnerability, June 28, 2004</p>
<p>rsync 2.6.2 and prior</p> <p>Debian</p> <p>SuSE</p> <p>Trustix</p>	<p>A vulnerability exists in rsync when running in daemon mode with chroot disabled. A remote user may be able read or write files on the target system that are located outside of the module's path. A remote user can supply a specially crafted path to cause the path cleaning function to generate an absolute filename instead of a relative one. The flaw resides</p>	<p>Rsync Input Validation Error in sanitize_path() May Let Remote Users Read or</p>	<p>High</p>	<p>SecurityTracker 1010940, August 12, 2004</p> <p>rsync August</p>

	<p>in the sanitize_path() function.</p> <p>Updates and patches are available at: http://rsync.samba.org/</p> <p>SuSE: http://www.suse.de/de/security/2004_26_rsync.html</p> <p>Debian: http://www.debian.org/security/2004/dsa-538</p> <p>Trustix: http://www.trustix.net/errata/2004/0042/</p> <p>We are not aware of any exploits for this vulnerability.</p>	Write Arbitrary Files		2004 Security Advisory
Silicon Graphics SGI IRIX 6.5.x, CDE 5.3.4	<p>A buffer overflow vulnerability exist in the libDtHelp module and a double-free vulnerability exists in the dtlogin module which a malicious user can use to gain root access.</p> <p>Upgrade to CDE 5.3.4 available at: ftp://patches.sgi.com/support/free/security/patches/6.5.25/</p> <p>We are not aware of any exploits for this vulnerability.</p>	SGI IRIX CDE Multiple Vulnerabilities CVE Names: CAN-2003-0834 CAN-2004-0368	Medium	SGI Security Advisory, 20040801-01-P, August 3, 2004
Sourceforge.net Gentoo Linux Pavuk 0.x	<p>Multiple vulnerabilities exist which could allow a malicious user to run arbitrary code. The vulnerabilities are caused due to boundary errors within the handling of digest authentication.</p> <p>Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200407-19.xml</p> <p><i>Exploit script has been published.</i></p>	Pavuk Digest Authentication Buffer Overflow Vulnerabilities	High	Gentoo Security Advisory, GLSA 200407-19 / Pavuk Release Date July 26, 2004 <i>SecurityFocus, August 7, 2004</i>
sox.sourceforge.net Fedora Mandrakesoft Gentoo Conectiva RedHat SoX 12.17.4, 12.17.3, and 12.17.2	<p>Multiple vulnerabilities exist that could allow a remote malicious user to execute arbitrary code This is due to boundary errors within the "st_wavstartread()" function when processing ".WAV" file headers and can be exploited to cause stack-based buffer overflows. Successful exploitation requires that a user is tricked into playing a malicious ".WAV" file with a large value in a length field.</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:076</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200407-23.xml</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-409.html</p> <p><i>Exploit script has been published.</i></p>	SoX ".WAV" File Processing Buffer Overflow Vulnerabilities CVE Name: CAN-2004-0557	High	Secunia, SA12175, 12176, 12180, July 29, 2004 SecurityTracker Alerts 1010800 and 1010801, July 28/29, 2004 Mandrakesoft Security Advisory MDKSA-2004:076, July 28, 2004 <i>PacketStorm, August 5, 2004</i>
SpamAssassin prior to 2.64	<p>A Denial of Service vulnerability exists in SpamAssassin. A remote user can send an e-mail message with specially crafted headers to cause a Denial of Service attack against the SpamAssassin service.</p> <p>Update to version (2.64), available at: http://old.spamassassin.org/released/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-06.xml</p> <p>We are not aware of any exploits for this vulnerability.</p>	SpamAssassin Lets Remote Users Deny of Service By Sending Malformed Messages	Low	SecurityTracker: 1010903, August 10, 2004
Team OpenFTPD OpenFTPD 0.30.2 prior to July 16, 2004, and prior versions	<p>A vulnerability exists that could allow a remote malicious user to execute arbitrary code on the target system. A remote authenticated user can send a specially crafted message to another FTP user to trigger a format string flaw and execute arbitrary code on the FTP server due to a flaw in 'misc/msg.c'.</p> <p>Update available at: http://www.openftpd.org:9673/openftpd/download_page.html</p> <p><i>Exploit script has been published.</i></p>	OpenFTPD Format String Flaw Lets Remote Authenticated Users Execute Arbitrary Code	High	VSA0402 - openftpd - void.at security notice, July 31, 2004 <i>PacketStorm, August 5, 2004</i>
xine-Project	<p>A buffer overflow vulnerability exists in xine in the processing of 'vcd://' protocol identifiers. A remote malicious user can execute arbitrary code on the target system. A remote malicious user can trigger a stack</p>	xine Buffer Overflow in Processing 'vcd'	High	SecurityTracker: 1010895, August 8, 2004

xine 0.99.2	<p>overflow in xine-lib by embedding a specially crafted source identifier within a playlist file, for example. When the target user plays the file, arbitrary code can be executed with the privileges of the target user.</p> <p>A patch is available via CVS at: http://sourceforge.net/mailarchive/forum.php?thread_id=5143955&forum_id=11923</p> <p>A Proof of Concept exploit has been published.</p>	Identifiers Lets Remote Users Execute Arbitrary Code	Open security advisory #6, August, 8, 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 AOL Instant Messenger (AIM) 5.5	<p>A buffer overflow vulnerability exists in America Online's Instant Messenger (AIM) which can allow remote malicious users to execute arbitrary code. The vulnerability specifically exists due to insufficient bounds checking on user-supplied values passed to the 'goaway' function of the AOL Instant Messenger 'aim:' URI handler.</p> <p>Upgrade to AIM beta version available at: www.aim.com</p> <p>Proof of Concept exploit script has been published.</p>	AOL Instant Messenger aim:goaway URI Handler Buffer Overflow Vulnerability	High	<p>iDEFENSE Security Advisory 08.09.04</p> <p>Secunia, SA12198, August 9, 2004</p> <p>US-CERT Vulnerability Note VU#735966, August 10, 2004</p>
Apache Software Foundation Apple Mandrake Trustix Apache 2.0.47 2.0.49	<p>A remote Denial of Service vulnerability exists in the 'ap_get_mime_headers_core()' function due to a failure to handle excessively long HTTP header strings.</p> <p>Patches available at: http://www.apache.org/dist/httpd/patches/apply_to_2.0.49/CAN-2004-0493.patch</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p> <p>Exploit scripts have been published.</p>	<p>Apache ap_escape_html Remote Denial of Service</p> <p>CVE Name: CAN-2004-0493</p>	Low	<p>Mandrakelinux Security Update Advisory, MDKSA-2004:064, June 29, 2004</p> <p>Trustix Security Advisory, TSL-2004-0038, June 29, 2004</p> <p>SecurityFocus, August 6, 2004</p>
Apple Apple Macintosh OS X Safari 1.x	<p>Apple has issued a security update for Mac OS X, which fixes various vulnerabilities. Multiple vulnerabilities in libpng that can be exploited to cause a Denial of Service or compromise a user's system; a vulnerability in the Safari browser can be used to steal sensitive information from forms; a vulnerability in the processing of network traffic that can be used to cause a DoS. The attack known as the "Rose Attack" will cause the system to use too much system resources resulting in DoS.</p> <p>Apply Security Update 2004-08-09.</p> <p>Mac OS X 10.3.5: http://wsidcar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04216&platform=osx&method=sa/SecUpd2004-08-09Pan.dmg</p> <p>Mac OS X 10.2.8: http://wsidcar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04285&platform=osx&method=sa/SecUpd2004-08-09Jag.dmg</p> <p>We are not aware of any exploits for this vulnerability.</p> <p>See also Multiple Vulnerabilities in libpng.</p>	Mac OS X Security Update Fixes Multiple Vulnerabilities	High	Secunia, SA12249, August 10, 2004
CuteNews 1.3.1	<p>An input validation vulnerability exists in CuteNews, which can be exploited by a remote malicious user to conduct cross-site scripting attacks. Input passed to the "archive" parameter in "show_archives.php" is not sanitized properly before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected website by tricking the user into visiting a malicious website or follow a specially crafted link.</p> <p>No solution is available at this time.</p> <p>A Proof of Concept exploit has been published.</p>	CuteNews "archive" Parameter Cross-Site Scripting Vulnerability	High	Secunia, SA12260, August 16, 2004
Concurrent	A vulnerability exists in Concurrent Versions System (CVS) in which a	CVS	Low	iDEFENSE Security

Versions Systems (CVS) 1.11	<p>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.</p> <p>Upgrade to version 1.11.17 or 1.12.9 available at: https://www.cvshome.org/</p> <p>A Proof of Concept exploit has been published.</p>	<p>Undocumented Flag Information Disclosure Vulnerability</p> <p>CVE Name: CAN-2004-0778</p>		Advisory 08.16.04
Indonesia.Com eNdonesia 8.3	<p>Input verification vulnerabilities exist that could allow a remote malicious user to conduct cross-site scripting attacks or determine the installation path. The software does not properly filter HTML code from user-supplied input in the "query" parameter. A remote user can submit a request with certain invalid parameters to cause the system to display the installation path.</p> <p>No solution is available at this time.</p> <p>A Proof of Concept exploit has been published.</p>	<p>eNdonesia 'mod.php' Input Validation Vulnerability in Search 'query' Parameter Permits Cross-Site Scripting Attacks</p>	High	SecurityTracker: 1010865, August 4, 2004
GoScript 2.0	<p>An input validation vulnerability exists in GoScript that could allow a remote user to execute arbitrary commands on the target system. The 'go.cgi' script does not validate user-supplied input. A remote user can supply a specially crafted URL to execute operating system commands on the target system with the privileges of the target web service.</p> <p>No solution is available at this time.</p> <p>A Proof of Concept exploit has been published.</p>	<p>GoScript Input Validation Hole Lets Remote Users Execute Arbitrary Commands</p>	High	SecurityTracker 1010865, August 4, 2004
IBM IBM Tivoli Access Manager for e-business 3.x, 4.x, 5.x	<p>An input validation vulnerability exists in IBM Tivoli Access Manager for e-business, which could allow a remote malicious user to conduct cross-site scripting attacks and gain control over an affected system.</p> <p>Patch as appropriate at: http://www.ibm.com/support/us/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>IBM Tivoli Access Manager HTTP Response Splitting Vulnerability</p>	High	Secunia, SA12093, August 9, 2004
Juniper Juniper Networks NetScreen firewalls with SSHv1 enabled - ScreenOS prior to 5.0.0r8	<p>A vulnerability exists in ScreenOS in the processing of SSHv1 management connections that could allow a remote malicious user cause the device to crash. If SSH version 1 is enabled on the target device, a remote user can connect to the management port and cause the device to hang or to crash and reboot. Authentication is not required.</p> <p>Updates available at: http://www.juniper.net/support/</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>NetScreen Firewalls ScreenOS Can Be Crashed By Remote Users Due to an SSHv1 Implementation Bug</p>	Low	<p>Juniper Networks NetScreen Advisory 59147, August 3, 2004</p> <p>SecurityTracker 1010848, August 3, 2004</p> <p>US-CERT Vulnerability Note VU#749870, August 13, 2004</p>
Mark Burgess Cfengine 2.0.0 to 2.1.7p1.	<p>Input validation and buffer overflow vulnerabilities exist in Cfengine which could allow a remote malicious user to execute arbitrary code or cause a DoS (Denial of Service). The vulnerabilities are caused due to insufficient input validation and a boundary error in the cfservd daemon when processing authentication requests. The problems lies in the AuthenticationDialogue()" function, which is responsible for performing RSA authentication and key agreement.</p> <p>Update to version 2.1.8 available at: http://www.cfengine.org/mirrors.html</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-08.xml</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Cfengine RSA Authentication Heap Corruption</p>	High	Core Security Technologies Advisory, Advisory ID: CORE-2004-0714, August 9, 2004
Matt Johnston Dropbear SSH Server 0.42	<p>A vulnerability exists that could allow a remote malicious user to execute arbitrary code. This vulnerability is caused due to freeing of uninitialized variables in the DSS verification code.</p> <p>Update to version 0.43 available at: http://matt.ucc.asn.au/dropbear/</p> <p>Exploit scripts have been published.</p>	<p>Dropbear SSH Server DSS Verification Vulnerability</p>	High	<p>Secunia, SA12153, July 26, 2004</p> <p>Dropbear Security Update</p> <p>Packetstorm, August 4, 2004</p>
moodle.org	<p>An input validation vulnerability was reported in Moodle in 'post.php' in</p>	<p>Moodle Input</p>	High	SecurityTracker,

Moodle versions prior to 1.3	<p>which a remote malicious user can conduct cross-site scripting attacks. 'post.php' does not properly filter HTML code from user-supplied input in the reply variable. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Moodle software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.</p> <p>Update to version 1.3 or above available at: http://moodle.org/mod/resource/view.php?id=8</p> <p>A Proof of Concept exploit has been published.</p>	Validation Flaw in 'post.php' in reply Variable Permits Cross-Site Scripting Attacks		1010893, August 7, 2004
<p>Mozilla Organization Mandrakesoft Slackware</p> <p>Mozilla 1.7 and prior; Firefox 0.9 and prior; Thunderbird 0.7 and prior</p>	<p>Multiple vulnerabilities exist in Mozilla, Firefox, and Thunderbird that could allow a malicious user to conduct spoofing attacks, compromise a vulnerable system, or cause a Denial of Service. These vulnerabilities include buffer overflow, input verification, insecure certificate name matching, and out-of-bounds reads.</p> <p>Upgrade to the latest version of Mozilla, Firefox, or Thunderbird available at: http://www.mozilla.org/download.html</p> <p>Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.667659</p> <p>Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:082</p> <p>We are not aware of any exploits for this vulnerability.</p>	Mozilla Multiple Vulnerabilities	High	Secunia, SA10856, August 4, 2004
<p>Nokia</p> <p>Nokia IPSO 3.5, 3.5.1, 3.6, 3.7, 3.7.1, 3.8</p>	<p>A vulnerability exists in Nokia IPSO, which can be exploited by a malicious user to cause a Denial of Service.</p> <p>Update to the latest builds.</p> <p>We are not aware of any exploits for this vulnerability.</p>	Nokia IPSO Denial of Service Vulnerability	Low	<p>Secunia, SA12280, August 12, 2004</p> <p>Nokia Knowledge Base, Resolution 21008</p>
<p>Opera Software</p> <p>Opera 7.53</p>	<p>A spoofing vulnerability exists that could be exploited by a malicious user to conduct phishing attacks against a user. Opera fails to update the address bar if a web page is opened using the "window.open" function and then "replaced" using the "location.replace" function. This causes Opera to display the URL of the first website while loading the content of the second website.</p> <p>Update to 7.54 available at: http://www.opera.com/download/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-05.xml</p> <p><i>A Proof of Concept exploit has been published.</i></p>	Opera Browser Spoofing Vulnerability	High	<p>Secunia, SA12162, July 27, 2004</p> <p>Gentoo SA, GLSA 200408-05 / Opera, August 05, 2004</p> <p><i>GreyMagic Security Advisory GM#008-OP, August 5, 2004</i></p>
<p>PHP Foundry</p> <p>Jetbox One 2.0.8</p>	<p>An input validation vulnerability exists in Jetbox One that could allow users with "Author" privileges in "IMAGES" to upload arbitrary files including PHP code. The vulnerability exists because the type of file being uploaded is not verified as a valid image file e.g. GIF, JPEG. Once uploaded, the malicious user is then able to request the file, which will be interpreted by the JetboxOne application.</p> <p>Also, JetboxOne does not encrypt information in the account information database. Any user with the ability to query the database may be able to view confidential account information.</p> <p>No vendor solution is available.</p> <p>A Proof of Concept exploit has been published.</p>	<p>JetBoxOne CMS Arbitrary File Upload Vulnerability</p> <p>JetBoxOne Leaves Account Database Unencrypted</p>	High	<p>Secunia, SA12230, August 5, 2004</p> <p>US-CERT Vulnerability Note #417408, August 13, 2004</p> <p>US-CERT Vulnerability Note #58670, August 13, 2004</p>
<p>Phpnuke.org</p> <p>PHP-Nuke 7.x</p>	<p>An input verification vulnerability exists in PHP-Nuke which a malicious user can exploit to conduct cross-site scripting attacks. User input passed to the search box in the following modules is not sanitized before being returned to users: Web_Links, Journal, Stories Archive, Topics Archive.</p> <p>No vendor solution is available.</p> <p>A Proof of Concept exploit has been published.</p>	PHP-Nuke Search Box Cross-Site Scripting Vulnerabilities	High	<p>Secunia, SA12271, August 11, 2004</p> <p>SystemSecure.org, Advisory SS#23072004</p>
<p>PluggedOut</p> <p>Blog 1.6 alpha and prior</p>	<p>An input validation vulnerability exists that could allow a remote malicious user to conduct cross-site scripting attacks. The software does not filter HTML code from user-supplied input in the 'blogid' variable. The malicious user can access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted</p>	PluggedOut Blog Input Validation Hole in 'blogid'	High	VulnWatch, August 7, 2004

	<p>by the target user via web form to the site, or take actions on the site acting as the target user.</p> <p>No vendor solution is available.</p> <p>A Proof of Concept exploit has been published.</p>			
<p>PNG Development Group</p> <p>Conectiva</p> <p>Debian</p> <p>Fedora</p> <p>Gentoo</p> <p>Mandrakesoft</p> <p>RedHat</p> <p>SuSE</p> <p>Sun Solaris</p> <p>HP-UX</p> <p>GraphicsMagick</p> <p>ImageMagick</p> <p>Slackware</p> <p>libpng 1.2.5 and 1.0.15</p>	<p>Multiple vulnerabilities exist in the libpng library which could allow a remote malicious user to crash or execute arbitrary code on an affected system. These vulnerabilities include:</p> <ul style="list-style-type: none"> libpng fails to properly check length of transparency chunk (tRNS) data, libpng png_handle_iCCP() NULL pointer dereference, libpng integer overflow in image height processing, libpng png_handle_sPLT() integer overflow, libpng png_handle_sBIT() performs insufficient bounds checking, libpng contains integer overflows in progressive display image reading. <p>If using original, update to libpng version 1.2.6rc1 (release candidate 1) available at: http://www.libpng.org/pub/png/libpng.html</p> <p>Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000856</p> <p>Debian: http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00139.html</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200408-03.xml</p> <p>Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:079</p> <p>RedHat http://rhn.redhat.com/</p> <p>SuSE: http://www.suse.de/de/security/2004_23_libpng.html</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>Sun Solaris: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert/57617</p> <p>HP-UX: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01065</p> <p>GraphicsMagick: http://www.graphicsmagick.org/www/download.html</p> <p>ImageMagick: http://www.imagemagick.org/www/download.html</p> <p>Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.439243</p> <p>Yahoo: http://messenger.yahoo.com/</p> <p>A Proof of Concept exploit has been published.</p>	<p>Multiple Vulnerabilities in libpng</p> <p>CVE Names: CAN-2004-0597 CAN-2004-0598 CAN-2004-0599</p>	<p>High</p>	<p>US-CERT Technical Cyber Security Alert TA04-217A, August 4, 2004</p> <p>US-CERT Vulnerability Notes VU#160448, VU#388984, VU#817368, VU#236656, VU#477512, VU#286464, August 4, 2004.</p>
<p>QuiXplorer - Quick (PHP) Explorer 2.3 and prior</p>	<p>A directory traversal vulnerability was reported in QuiXplorer. A remote user can view files on the target system. QuiXplorer does not properly filter user-supplied input in the 'item' parameter. A remote user can submit a specially crafted request to view files located anywhere on the target system.</p> <p>Update to 2.3.1, available at: http://sourceforge.net/project/showfiles.php?group_id=72517</p> <p>A Proof of Concept exploit has been published.</p>	<p>QuiXplorer Input Validation Hole in 'item' Parameter Discloses Files to Remote Users</p>	<p>Medium</p>	<p>SecurityTracker 1010954, August 15, 2004</p>
<p>Simon Tatham</p> <p>Gentoo</p> <p>PuTTY 0.54 and previous</p>	<p>Input validation and buffer overflow vulnerabilities exist in PuTTY that could allow a remote malicious user to execute arbitrary code. By sending specially crafted packets to the client during the authentication process, a malicious user is able to compromise and execute arbitrary code on the machine running PuTTY or PSCP.</p>	<p>PuTTY System Compromise Vulnerability</p>	<p>High</p>	<p>Core Security Technologies Advisory number CORE-2004-0705</p>

	<p>Update to version 0.55 available at: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html</p> <p>Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200408-04.xml</p> <p>A Proof of Concept exploit has been published.</p>			
<p>Sun Microsystems Sun Solaris 7, 8, 9</p>	<p>A vulnerability has been reported in Solaris, which can be exploited by malicious people to cause a Denial of Service. The vulnerability is caused due to an unspecified error within the processing of XDMCP requests. Successful exploitation crashes the X Display Manager (xdm).</p> <p>Apply patches or vendor workaround available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57619</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Sun Solaris XDMCP Parsing Vulnerability</p>	<p>Low</p>	<p>Sun Alert ID: 57619, August 9, 2004</p> <p>US-CERT Vulnerability Note VU#139504, August 11, 2004</p>
<p>The Webmaster Guide, Inc. Board Power v2.04 PF</p>	<p>An input validation vulnerability exists in Board Power forum could allow a remote malicious user to conduct cross-site scripting attacks and execute arbitrary code. Board Power fails to filter malicious content passed into the "action" parameter of icq.cgi. This could be used to "sniff" sensitive data from within the web page, including passwords, credit card numbers, and any arbitrary information the user inputs. Likewise, information stored in cookies can be stolen or corrupted.</p> <p>No solution is available at this time.</p> <p>A Proof of Concept exploit has been published.</p>	<p>Board Power forum contains cross-site scripting vulnerability</p>	<p>High</p>	<p>US-CERT Vulnerability Note VU#744590, August 5, 2004</p>
<p>Thompson SpeedTouch Home ADSL Modem firmware version GV8BAA3.270 (1003825) and earlier</p>	<p>A design error vulnerability exists in Thompson's SpeedTouch Home ADSL modem that could allow a malicious user to spoof TCP traffic on behalf of the device. The problem specifically exists due to the predictable nature of the TCP Initial Sequence Number (ISN) generator on the device.</p> <p>No vendor solution is available at this time.</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>Thompson SpeedTouch Home ADSL Modem Predictable TCP ISN Generation</p> <p>CVE Name: CAN-2004-0641</p>	<p>Medium</p>	<p>DEFENSE Security Advisory, August 5, 2004</p> <p>SecuriTeam, August 9, 2004</p>
<p>Volker Rattel phpBB Fetch All 2.0.10 and 2.0.11</p>	<p>An input verification vulnerability exists in phpBB Fetch All that could allow a malicious user to pass malicious SQL statements to the underlying function. Successful exploitation could result in compromise of the application, disclosure or modification of data or may permit a malicious user to exploit vulnerabilities in the underlying database implementation.</p> <p>Upgrade to 2.0.12 available at: http://prdownloads.sourceforge.net/phpbbfetchall/phpbb_fetch_all-2.0.12.zip?download</p> <p>No exploit code required.</p>	<p>phpBB Fetch All SQL Injection Vulnerability</p>	<p>High</p>	<p>SecurityFocus, August 4, 2004</p>
<p>vRating 4.0, 4.01</p>	<p>A disclosure vulnerability exists in vRating. A remote malicious user can view and edit the 'settings.php' file with a specially crafted URL. A malicious user can also access the 'admin' directory to gain access to the administrative interface.</p> <p>No solution is available at this time.</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>vRating Discloses Sensitive Information and Grants Administrative Access to Remote Users</p>	<p>Medium</p>	<p>SecurityTracker 1010951, August 13 2004</p>
<p>WackoWiki 3.x</p>	<p>An input validation vulnerability exists in WackoWiki in which a malicious user can exploit to execute conduct cross-site scripting attacks and arbitrary HTML and script code in a user's browser session in context of an affected website.</p> <p>Upgrade to version R4 available at: http://wackowiki.com/WackoDownload/InEnglish</p> <p>We are not aware of any exploits for this vulnerability.</p>	<p>WackoWiki textsearch Cross- Site Scripting Vulnerability</p>	<p>High</p>	<p>Secunia, SA12209, August 4, 2004</p>
<p>Xavier Cirac Shuttle FTP Suite 3.2</p>	<p>An input verification vulnerability exists in Shuttle FTP Suite, which can be exploited by a malicious user to read or place files in arbitrary locations on a vulnerable system. Arguments passed to certain commands are not properly verified. This can be exploited to access and write files outside the FTP root using the classical directory traversal character sequence "../" or absolute paths.</p> <p>No solution is available at this time.</p>	<p>Shuttle FTP Suite Directory Traversal Vulnerability</p>	<p>Medium</p>	<p>Secunia, SA12270, August 11, 2004</p>

We are not aware of any exploits for this vulnerability.

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

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing.

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

Date of Script (Reverse Chronological Order)	Script name	Script Description
August 17, 2004	SpecificMAIL.theft.txt	A freeware spam filter for Outlook and Outlook Express that is extremely intrusive and acts more as spyware than a useful utility to users.
August 16, 2004	proc_kmem_dump.c	Script that exploits the Linux Kernel Proc_kmem_dump vulnerability.
August 14, 2004	aimAway.c	Proof of concept exploit for AOL Instant Messenger aim:goaway URI Handler Buffer Overflow Vulnerability.
August 13, 2004	ethereal-0.10.6.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
August 13, 2004	gv-exploit.c	Script that exploits the gv Local Buffer Overflow vulnerability.
August 13, 2004	netgearDG834G.txt	The Netgear DG834G has a hardcoded root password of zebra and a debug mode that allows for an immediately available rootshell.
August 13, 2004	priv8afp.pl	Remote root exploit for Mac OS X Apple Filing Protocol Buffer Overflow vulnerability.
August 12, 2004	aircrack-1.1.tgz	An 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered. It implements the standard FMS attack along with some optimizations, thus making the attack much faster compared to other WEP cracking tools.
August 12, 2004	freedom.c	Remote CVS exploit for the Double free() Heap Overflow vulnerability.
August 12, 2004	mercantec_softcart.pm	Exploit for the Mercantec Softcart CGI Buffer Overflow vulnerability.
August 12, 2004	pngslap.c	Script that exploits the Libpng Buffer Offset Calculation Overflow vulnerability.
August 12, 2004	rkhunter-1.1.5.tar.gz	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
August 11, 2004	0x4553_Exorcist.tar.gz	A tool that can be considered an anti-anti-pttrace utility that unlocks the ptrace_traceme guard of a binary.
August 11, 2004	0x4553_Scorpion.tar.gz	Tool for infecting statically linked ELF binaries.
August 11, 2004	0x4553-Static_Infecting.html	White paper that discusses a method of infecting statically linked ELF binaries.
August 11, 2004	c030224-001.txt	Detailed exploit details for the ServerMask Header Identification vulnerability.
August 11, 2004	framework-2.2.tar.gz	The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code. This release includes 18 exploits and 27 payloads.
August 11, 2004	OllyExp.c	Script that exploits the OllyDbg Debugger Messages Format String vulnerability.
August 10, 2004	linuxKernelFileOffsetPointerHandlingExploit.c	Exploit for the Linux Kernel File 64-Bit Offset Pointer Handling Kernel Memory Disclosure vulnerability.
August 9, 2004	Xines_Mine.c	Script that exploits the Xine Buffer Overflow vulnerability.

August 9, 2004	yapig_script_injection.php	Exploit for the YaPiG Remote Server-Side Script Execution vulnerability.
August 8, 2004	servulocal.c	Script that exploits the RhinoSoft Serv-U FTP Server Default Administration Account vulnerability.
August 7, 2004	pavuk.c	Script that exploits the Pavuk Digest Authentication Buffer Overflow Vulnerabilities.
August 7, 2004	pavukWebSpider.c	Script that exploits the Pavuk Digest Authentication Buffer Overflow Vulnerabilities.
August 6, 2004	apache-dos.pl	Perl script that exploits the Apache ap_escape_html Remote Denial of Service vulnerability.
August 6, 2004	apacheEscapeHeaderD0SExploit.c	Script that exploits the Apache ap_escape_html Remote Denial of Service vulnerability.
August 5, 2004	aircrack-1.0.tgz	An 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered.
August 5, 2004	bjd361exp.cpp	Proof of Concept exploit for the BlackJumboDog FTP Buffer Overflow vulnerability.
August 5, 2004	C-MD5.tar.bz2	MD5 Brute Force Tool that tests the security of MD5 passwords by attempting to brute force them.
August 5, 2004	evil_song.py	Exploit for the SoX ".WAV" File Processing Buffer Overflow Vulnerability.
August 5, 2004	hoagie_openftpd.c	Remote root exploit for OpenFTPD Format String vulnerability.
August 5, 2004	HOD-ms04022-task-expl.c	Exploit for the Microsoft Windows Task Scheduler Remote Buffer Overflow vulnerability.
August 5, 2004	hydra-4.2-src.tar.gz	A high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more.
August 5, 2004	isec-0016-procleaks.txt	Exploit for the Linux Kernel 64-bit to 32-bit File Offset Conversion vulnerability.
August 5, 2004	mailEnable.txt	Exploit for the MailEnable Content-Length Denial Of Service vulnerability.
August 5, 2004	openf.c	Remote root exploit for OpenFTPD Format String vulnerability.
August 5, 2004	pocExploitEtherealINSProtocolVuln.c	Proof of Concept exploit for the Ethereal iSNS Protocol Denial of Service vulnerability.
August 4, 2004	drop-root.c	Script that exploits the Dropbear SSH Server DSS Verification Vulnerability.
August 4, 2004	FreeWebChat[Mir]DoS-po.cc	Script that exploits the Free Web Chat Denial Of Service Vulnerabilities.
August 4, 2004	FreeWebChat_ir_RC_poc.java	Exploit for the Free Web Chat Denial Of Service Vulnerabilities.
August 4, 2004	libpn.gc	Script that exploits the LibPNG Graphics Library Denial of Service vulnerability.
August 4, 2004	linuxKernelFileOffsetPointerHandlingExploit.c	Script that exploits the Linux Kernel File 64-Bit Offset Pointer Handling Kernel Memory Disclosure Vulnerability.
August 4, 2004	soxWAVfilebufferoverflowexploit.tc	Exploit for the SoX ".WAV" File Processing Buffer Overflow Vulnerability.

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

Trends

- Seven months since the W32/Bagle mass-mailing virus first appeared on the Internet, US-CERT continues to see new variants appearing and many variants (new and old) continuing to spread. Many variants of W32/Beagle are known to open a backdoor on an infected system which can lead to further exploitation by remote malicious users.

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

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 during the latest three months), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	W32/Netsky-P	Win32 Worm	Stable	March 2004
2	W32/Zafi-B	Win32 Worm	Stable	June 2004
3	W32/Netsky-Q	Win32 Worm	Increase	March 2004
4	W32/Netsky-D	Win32 Worm	Slight Increase	March 2004
5	W32/Netsky-B	Win32 Worm	Slight Increase	February 2004
6	W32/Netsky-Z	Win32 Worm	Decrease	April 2004
7	W32/Bagle-AA	Win32 Worm	Decrease	April 2004
8	W32/MyDoom-M	Win32 Worm	New to Table	July 2004
9	W32/MyDoom-O	Win32 Worm	New to Table	July 2004
9	I-Worm.Bagle.z	Win32 Worm	New to Table	April 2004
9	I-Worm.Bagle.AI	Win32 Worm	New to Table	July 2004
10	Worm_Sasser.B	Win32 Worm	Decrease	April 2004
10	W32/Netsky-C	Win32 Worm	Return to Table	March 2004
10	W32/Mydoom.s@MM	Win32 Worm	New to Table	August 2004
10	W32/Mydoom.q	Win32 Worm	New to Table	August 2004

New Viruses / Trojans

Viruses or Trojans Considered to be a High Level of Threat

- [Brador/Bardoor](#) These are the first known backdoor Trojans for the Pocket PC hand-held devices. They send the IP address of the infected handheld to the malicious user and opens various TCP ports. Brador only affects Windows Mobile 2003 (Pocket PC 2003 and Windows CE 4.2) and ARM-based devices.

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
Agobot-LT	WORM_AGOBOT.OC W32/Agobot-LT	Win32 Worm
Amus.A	I-Worm.Amus.a W32.Amus.A@mm W32/Amus.A.worm Win32.Amus.A WORM_AMUS.A	Win32 Worm
Backdoor.Beasty.I		Trojan
Backdoor-CFB	W32/Backdoor-CFB	Win32 Worm
Bardoor	Backdoor.Bardor.A	WinCE Trojan
Bck/Surila.B	Surila.B W32/Mydoom.R	Trojan
Brador	Brador.A Backdoor.WinCE.Brador.a Backdoor.Brador.A Bck/WinCE.Brador.A Troj/Brador-A WINCE_BRADOR.A WinCE/BackDoor-CHK	WinCE Trojan
Cata-A	VBS/Cata-A	Visual Basic Script Virus
Daqa.B	BackDoor-BDI Win32.Daqa.B	Win32 Worm

	Win32/Daqa.B.Trojan	
Daqa.C	BackDoor-BDI Win32.Daqa.C Win32/Daqa.C.Trojan	Win32 Worm
Doep-A	W32.Doep.A W32/Doep-A W32/Ourtime!p2p Worm.P2P.Doep.a WORM_DOEP.A	Win32 Worm
Downloader.Harnig		Trojan
Downloader.OG	Trj/Downloader.OG	Trojan: Adware Downloader
Febelneck-A	W32/Febelneck-A W32.Febelneck@mm Febelneck trojan I-Worm.Febelneck	Win32 Worm
Frear.A	Win32.Frear.A Win32/FriTear.A Worm.P2P.Delf.u Win32/Frear.A.Worm	Win32 Worm
JS/Zerolin		Java Script Trojan
Keylog-Melcarr		Trojan
Lovgate.AN	W32.Lovgate.AN@mm	Win32 Worm
MyDoom.R	W32/MyDoom-R W32/Mydoom.r@MM WORM_MYDOOM.R W32.Mydoom.P@mm	Win32 Worm
Myfip.A	W32.Myfip.A	Win32 Worm
Nachi.L	MS03-026 W32/Nachi.worm.m Win32.Nachi.L Win32/Nachi.L Worm.Win32.Welchia.l Worm/Nachi.S WORM_NACHI.L	Win32 Worm
Nachi-K	W32/Nachi-K W32/Nachi.worm.m Worm.Win32.Welchia.l W32.Welchia.gen	Win32 Worm
Padodor-L	Troj/Padodor-L	Trojan
PE_LOVGATE.E	Win32.Lovgate.AY	File Infector Virus
PWSteal.Perfectspy		Trojan: Spyware Installer
Reign.V	TrojanProxy.Win32.Agent.ag W32/Agent.T Win32.Reign.V Win32/Agent.T.DLL.Trojanbr Win32.Reign.W Win32/Reign.29227.Trojan Win32/TrojanProxy.Agent.AG	Win32 Worm
Saros	I-Worm.Saros.a Saros.A W32.Saros@mm W32/Saros@MM Win32.Saros.A WORM_SAROS.A CRYPT.WIN32 virus IW32/Saros-A	Win32 Worm
Sconato.A	Keylog-Sconato Trj/Sconato.A Troj/Sconato-A Trojan.ScoNato.A Trojan.Win32.Sconato.a	Trojan: Keylogger
Sdbot-LU	W32/Sdbot.worm.gen Backdoor.SdBot.nv BKDR_SDBOT.GEN W32/Sdbot-LU	Win32 Worm
Sndc.A	W32.IRCBot W32/Pcbot.A@p2p W32/Sndc.worm!p2p Win32.Sndc.A	Win32 Worm

	Win32/P2P.Sndc.Worm Worm.P2P.Krepper.c	
Startpage.FZ	StartPage-DU Trojan.Win32.StartPage.ix Win32.Startpage.FZ Win32/StartPage.IX	Win32 Worm
StartPage-EM		Trojan
SYMBOS_QDIAL.A	Mquito SymbOS/Mquito Trojan.Mquito SymbOS/QDial26	Trojan
Trj/Leritand.A	Leritand.A	Trojan
Trj/Leritand.B	Leritand.B	Trojan
Trj/Leritand.C	Leritand.C	Trojan
Troj/Bdoor-CHR	BackDoor-CHR BackDoor-CHR.sys	Trojan
Troj/CmjSpy-Z		Trojan
Troj/Daemoni-G		Trojan
Troj/Iefeat-K		Trojan
Troj/Mosqit-A		Trojan
Troj/Padodor-L		Trojan
Troj/ProxDrop-A		Trojan
TROJ_BAGLE.AC		Trojan
Trojan.Boxed.E		Trojan
Trojan.Cargao.B		Trojan
Trojan.Nullpos		Trojan
Trojan.StartPage.F	TROJ_STRTPAGE.CQ Troj/CWS-C StartPage-CQ.gen TrojanDownloader.Win32.Small.lc	Trojan
Trojan.StartPage.G		Trojan
VBS.Mywav@mm		Visual Basic Script Worm
W32/Agobot-LX	Win32/Agobot.3.ZQ W32/Gaobot.worm.pp	Win32 Worm
W32/Agobot-MA		Win32 Worm
W32/Agobot-ZX		Win32 Worm
W32/Annil-G	I-Worm.Annil.g	Win32 Worm
W32/Apribot-C	Backdoor.IRCBot.gen W32/Sdbot.worm.gen.m virus	Win32 Worm
W32/Bagle.aq@MM	HTML_BAGLE.AC I-Worm.Bagle.al W32.Beagle.AO@mm W32/Bagle-AQ W32/Bagle.AJ@mm W32/Bagle.AM.worm WORM_BAGLE.AC JS/IIWill JS/Dword.dr TR/RunMe.Dldr.1 W32/Bagle.aq@MM Bagle.AG	Win32 Worm
W32/Cali-A		Win32 Worm
W32/Gobot-C	Backdoor.IRC.Bot Backdoor.Gobot.s	Win32 Worm
W32/Lovgate-F		Win32 Worm
W32/MyDoom-Q	W32/Mydoom.q@MM W32/Evaman.c@MM	Win32 Worm
W32/MyDoom-R		Win32 Worm
W32/Neveg.b@MM	W32/Cali@MM	Win32 Worm
W32/Neveg.c@MM		Win32 Worm
W32/Rbot-FQ	Backdoor.Rbot.gen W32/Sdbot.worm.gen.g	Win32 Worm
W32/Rbot-FV		Win32 Worm
W32/Rbot-FY		Win32 Worm

W32/Rbot-GF	W32/Sdbot.worm.gen.k Backdoor.Rbot.af	Win32 Worm
W32/Sdbot-MH		Win32 Worm
Win32.Daqa.B	BackDoor-BDI Win32/Daqa.B.Trojan Win32/Daqa.C.Trojan Win32.Daqa.C	Trojan
WORM_ATAK.C		Internet Work
WORM_LOVGATE.E	HLLM.Lovgate.18 I-Worm.Win32.Lovgate.171520 Worm/Lovgate.BJ I-Worm.LovGate.ah Win32/Lovgate.AS	Internet Worm
WORM_RATOS.A	W32.Mydoom.Q@mm I-Worm.Win32.Ratos W32/Mydoom.s@MM W32/MyDoom-S Win32.Mydoom.S WORM_RATOS.A	Win32 Worm
WORM_SDBOT.LD		Internet Worm

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

Last updated August 18, 2004