



Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-18

September 8, 2003

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between August 19 and September 5, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
akpop3d ¹	Unix	akpop3d 0.4-0.6, 0.7-0.7.5	A vulnerability exists due to an error in the authentication code due to insufficient sanitization of usernames, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.synflood.at/akpop3d/akpop3d-0.7.6.tar.bz2	akpop3d Authentication Code	Medium	Bug discussed in newsgroups and websites.
AnalogX ²	Windows 95/98/NT 4.0/2000	Proxy 4.0-4.0 7, 4.10, 4.13, 4.14	A Cross-Site Scripting vulnerability exists when the proxy encounters a DNS lookup failure, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Proxy Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹ Secunia Security Advisory, SA9595, August 25, 2003.

² SecurityTracker Alert, 1007566, August 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Anderson Che ³	Windows	Avant Browser 8.0.2	A buffer overflow vulnerability exists due to insufficient checking of URL values, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Avant Browser Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Attila PHP ⁴	Windows, Unix	Attila PHP 3.0	An SQL injection vulnerability exists in the 'cook_id' parameter, which could let a remote malicious user obtain unauthorized privileged access.	No workaround or patch available at time of publishing.	Attila PHP Unauthorized Privileged Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
BEA Systems, Inc. ⁵	Unix	WebLogic Integration 8.1	A file system access vulnerability exists, which could let a remote malicious user obtain sensitive information.	Patch available at: ftp://ftpna.beasys.com/pub/releases/security/P001_WLI_BC81.zip	WebLogic Integration File System Access	Medium	Bug discussed in newsgroups and websites.
BitMover, Inc. ⁶	Windows, Unix	BitKeeper 2.0.1, 2.0.3-2.0.5, 2.1-2.1.5, 3.0, 3.0.1	A vulnerability exists in the trigger functionality due to an insecure default configuration, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	BitKeeper Insecure Configuration	High	Bug discussed in newsgroups and websites.
BProc ⁷	Unix	BProc 3.2.5	A vulnerability exists in Beowulf Distributed Process Space because IO redirection is set up with wrong permissions, which could let a malicious user delete arbitrary files.	Upgrade available at: http://sourceforge.net/projects/showfiles.php?group_id=24453	BProc Local Arbitrary File Deletion	Medium	Bug discussed in newsgroups and websites.
Castle Rock Computing ⁸	Windows	SNMPc 5.1, 6.0, 6.0.5, 6.0.8	A vulnerability exists due to the program performing user authentication client side in combination with the use of a weak password encryption, which could let a remote malicious user obtain supervisor access.	Patches available at: http://www.castlerock.com/download/fix821_608.zip	SNMPc v5/v6 Unauthorized Remote Privileged Access	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Check Point Software ⁹	Windows NT 4.0/2000	Firewall-1 4.0, SP1-SP8 4.1, SP1-SP4	An information leakage vulnerability exists when configured to use SecuRemote, which could let a remote malicious user obtain sensitive information.	Upgrade available at: www.checkpoint.com	Firewall-1 SecuRemote Information Leakage	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

³ Zud Security Team Advisory, August 22, 2003.

⁴ Bugtraq, August 26, 2003.

⁵ BEA Security Advisory, BEA 03-37.00, August 27, 2003.

⁶ SySS Security Advisory, August 19, 2003.

⁷ Secunia Advisory, SA9625,m August 28, 2003.

⁸ SecurityTracker Alert, 1007585, August 27, 2003.

⁹ IRM Security Advisory No. 007, September 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ¹⁰ <i>Upgrade now available</i> ¹¹	Multiple	VoIP Phone CP-7910 3.0-3.2, CP-7940 3.0-3.2, CP-7960 3.0-3.2	A remote Denial of Service vulnerability exists when a malicious user submits a spoofed ARP message.	<i>Upgrade now available at:</i> http://www.cisco.com/univerd/cc/td/doc/product/voice/c_ipphon/english/ipp7905g/relnotes/reInt3_3.htm#96716	Cisco 7900 Series VoIP Phone Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems ^{12, 13} <i>Upgrades & patches now available</i> ¹⁴	Multiple	Cisco Works CD1 1st Edition-5th Edition, Common Management Foundation 2.0, 2.1, Resource Manager 1.0, 1.1, Resource Manager Essentials 2.0-2.2	Several vulnerabilities exist: a vulnerability exists in the default configuration because the guest account is enabled with a blank password, which could let a malicious user circumvent authentication to obtain unauthorized administrative access; and a vulnerability exists when a specially crafted URL is submitted, which could let a remote malicious user execute arbitrary code.	<u>Workaround:</u> Cisco recommends disabling the Guest account as a workaround for the authentication bypass vulnerability until patches are available. <i>Upgrades are available to Cisco customers via the Product Upgrade Tool. Patches are also available to Cisco Customers for CMF 2.0 and 2.1 from Cisco's Software Center at:</i> http://www.cisco.com/warp/public/707/cisco-sa-20030813-cmf.shtml	CiscoWorks Common Management Foundation Administrative Authentication Bypass & Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁰ SecurityFocus, August 12, 2003.

¹¹ SecurityFocus, August 26, 2003.

¹² Portcullis Security Advisory, August 13, 2003.

¹³ Cisco Security Advisory, 44502, August 13, 2003.

¹⁴ SecurityFocus, August 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Emule, Imule, xMule ¹⁵ <i>Exploits published</i> ¹⁶	Unix	Emule 0.29a, 0.27c, 0.27b, 0.27, EMule+ 1.0, Imule 1.2.1, 1.3.1, xMule 1.4.2, 1.4.3, 1.5.4	Several vulnerabilities exist: a format string vulnerability exists in 'OP_SERVERMESSAGE' when a specially crafted message value is submitted to the connected target client, which could let a remote malicious user execute arbitrary code; a heap overflow vulnerability exists in the processing of the 'OP_SERVERIDENT' message, which could let a remote malicious user execute arbitrary code; a vulnerability exists because a server can be added to the network with a specially crafted server name containing format string characters, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists when a specially crafted sequence of packets is submitted, which could let a remote malicious user execute arbitrary code.	Update to eMule 0.30a available at: http://www.emule-project.net/index.php?s=downloads xMule version 1.4.3 (stable) has been released. However, it only fixes the Denial of Service and the packet sequence vulnerabilities. Imule is no longer supported.	eMule/Imule/xMule Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. <i>Proofs of Concept exploits have been published.</i>
eNdonesia ¹⁷	Windows, Unix	eNdonesia 8.2	A Cross-Site Scripting and path disclosure vulnerability exists in the 'mod.php' script, which could let a remote malicious user execute arbitrary HTML or script code or obtain sensitive information.	No workaround or patch available at time of publishing.	eNdonesia Cross-Site Scripting & Path Disclosure	Medium High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
ezboard ¹⁸	Multiple	ezboard	A Cross-Site Scripting vulnerability exists in the 'invitefriends.php3' script due to insufficient sanitization of user-supplied URI parameters, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Ezboard Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Fasoo.com ¹⁹	Windows	Wrapsody Viewer 3.0	A vulnerability exists in the digital rights management file wrapper, which could let a malicious user bypass copy-and-paste access restrictions.	Updates available at: http://www.wrapsody.co.kr/viewer.asp (Korean Version) http://eng.wrapsody.co.kr/viewer.asp (English Version)	Wrapsody View Copy And Paste Access Restrictions Bypass	Medium	Bug discussed in newsgroups and websites.

¹⁵ e-matters GmbH Security Advisory, August 18, 2003.

¹⁶ SecurityFocus, August 29, 2003.

¹⁷ Secunia Advisory, SA9622/, August 27, 2003.

¹⁸ SecurityFocus, September 1, 2003.

¹⁹ STG Security Advisory, SSA-20030902-04, September 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Floosietek ²⁰	Windows	FTGatePro 1.22 (1331)	Several vulnerabilities exist: a path disclosure vulnerability exists which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists in the 'index.fts' script due to insufficient validation, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists because the POP3 service returns different replies depending on whether a username is valid or invalid, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FTGatePro Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Path Disclosure vulnerability can be exploited via a web browser. Exploit has been published for the Cross-Site Scripting vulnerability. There is no exploit code required for the POP3 information disclosure vulnerability.
GMOD ²¹	Windows, Unix	GBrowse 1.43, 1.45-1.47, 1.50	A Directory Traversal vulnerability exists due to insufficient validation of user-supplied input to the 'help' parameter, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://prdownloads.sourceforge.net/gmod/Generic-Genome-Browser-1.53.tar.gz?download	GBrowse Help Parameter Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
GNU ²²	Unix	Whois 4.5.7, 4.6.6	A buffer overflow vulnerability exists when handling command line parameters of excessive length, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Whois Client Command Line Buffer Overflow	High	Bug discussed in newsgroups and websites.
GtkFtpd ²³	Unix	GtkFtpd 1.0.2- 1.0.4	A buffer overflow vulnerability exists in the 'LIST' command due to insufficient bounds checking when handling user-supplied data, which could let a remote malicious execute arbitrary code.	No workaround or patch available at time of publishing.	GtkFtpd 'LIST' Command Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
HAURI Inc. ²⁴	Unix	ViRobot Linux Server 2.0	Multiple buffer overflow vulnerabilities exist due to boundary errors in various suid files, which could let a local/remote malicious user obtain elevated privileges and possibly execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	ViRobot Linux Server Buffer Overflows	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.

²⁰ SecurityTracker Alert, 1007605, September 2, 2003.

²¹ SecurityFocus, August 26, 2003.

²² Zone-h Security Team Advisory, ZH2003-25SA, August 22, 2003.

²³ Secunia Advisory, SA9629, August 28, 2003.

²⁴ Secure Network Operations, Inc. Security Advisory, SRT2003-08-11-0729, August 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company ²⁵	Unix	Compaq Tru64 5.1 b PK2 (BL22), 5.1 a PK5 (BL23), 5.1 a PK4 (BL21), 5.1 a PK3 (BL3), 5.1 a PK2 (BL2), 5.1 a PK1 (BL1), 5.1a	An authentication bypass vulnerability exists in the SSH implementation when RSA signatures are incorrectly processed, which could let a malicious user obtain sensitive information.	Workaround and patches available at: http://h30097.www3.hp.com/manage/download.html#cm a http://h30097.www3.hp.com/internet/download.htm	Tru64 SSH RSA Key Potential Authentication Bypass	Medium	Bug discussed in newsgroups and websites.
Ideal Science, Inc. ²⁶	Windows	IdealBB 1.4.9 Beta	A vulnerability exists in 'error.asp' 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.	IdealBB HTML Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
ISC ²⁷	Multiple	INN (InterNet News) 2.0	A format string vulnerability exists in the 'innfeed' binary, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	INN Format String	High	Bug discussed in newsgroups and websites.
KisMAC ²⁸	Mac OS X	KisMAC 0.05d	Multiple vulnerabilities exist: a vulnerability exists in the 'viha_driver.sh,' 'macjack_load.sh,' and 'airojack_load.sh' scripts, which could let a malicious user change ownership of files or load arbitrary kernel modules; a vulnerability exists in the 'exchangeKernel.sh' script, which could let a malicious user overwrite the kernel; a vulnerability exists in the 'setuid_enable.sh' and 'setuid_disable.sh' scripts, which could let a malicious user change the ownership of arbitrary files; and a vulnerability exists in the 'viha_prep.sh' and 'viha_unprep.sh' scripts, which could let a malicious user execute arbitrary binary files with root privileges.	Update available at: http://freshmeat.net/releases/129083/	KisMAC Multiple Vulnerabilities CVE Names: CAN-2003-0703, CAN-2003-0704	High	Bug discussed in newsgroups and websites.

²⁵ Hewlett Packard Company Security Bulletin, SSRT3588, August 25, 2003.

²⁶ SecurityFocus, August 23, 2003.

²⁷ SecurityFocus, August 28, 2003.

²⁸ @stake, Inc. Security Advisory, August 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Laurent Duveau ²⁹	Windows, Unix	AldWeb MiniPortail 1.9, 2.0-2.3	A Cross-Site Scripting vulnerability exists because URLs with certain 'Ing' parameters are not handled properly, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	MiniPortail Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mark Osborne ³⁰	Unix	WIDZ 1.0 WIDZ 1.5	A vulnerability exists in the wireless IDS system due to insufficient validation of AP (Access Point) names in apmon' before supplying them to the 'system()' function, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	WIDZ Remote Root Compromise	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Martin Preis-huber ³¹ <i>Mandrake issues advisory</i> ³²	Unix	eroaster 2.0	A vulnerability exists due to insufficient security precautions when creating a temporary file for use as a lockfile, which could let a malicious user obtain elevated privileges.	Debian: http://security.debian.org/pool/updates/main/e/eroaster/ Mandrake: http://www.mandrakesecurity.net/en/advisories/	ERoaster Insecure Temporary File Creation CVE Name: CAN-2003-0656	Medium	Bug discussed in newsgroups and websites.
Microsoft ³³	Windows 95/98/ME/NT 4.0/2000, XP	Access 97, 2000, SR1, SP2&SP3, 2002, SP1&SP2	A buffer overflow vulnerability exists due to a flaw in the way that Snapshot Viewer validates parameters, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-038.asp	Access Snapshot Viewer ActiveX Control Remote Buffer Overflow CVE Name: CAN-2003-0665	High	Bug discussed in newsgroups and websites.
Microsoft ³⁴	Windows 95/98/SE/NT 4.0/2000, XP	Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1, Outlook 2000, SR1, SP1-SP3, Outlook 2002, SP1&SP2, Outlook XP	A Denial of Service vulnerability exists in the 'mshhtml.dll' library when malformed GIF images are handled.	No workaround or patch available at time of publishing.	Microsoft 'mshhtml.dll' Denial of Service	Low	Bug discussed in newsgroups and websites.

²⁹ Secunia Advisory, SA9621, August 27, 2003.

³⁰ Secure Network Operations Inc. Advisory, SRT2003-08-22-104, August 22, 2003.

³¹ Debian Security Advisory, DSA 366-1, August 6, 2003.

³² Mandrake Linux Security Update Advisory, MDKSA-2003:083, August 19, 2003.

³³ Microsoft Security Bulletin, MS03-038 V1.1, September 4, 2003.

³⁴ SecurityFocus, September 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ³⁵ <i>Another exploit published</i> ³⁶	Windows 95/98/ME/NT 4.0/2000/2003	Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1	Several vulnerabilities exist: a buffer overflow vulnerability exists because an object type returned from a web server is not properly identified, which could let a malicious user execute arbitrary code; and a vulnerability exists because an appropriate block on a file download dialog box is not implemented, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-020.asp	Microsoft Internet Explorer OBJECT Tag Buffer Overflow CVE Names: CAN-2003-0309, CAN-2003-0344	High	Bug discussed in newsgroups and websites. Exploit script has been published. <i>Another exploit script has been published.</i>
Microsoft ³⁷ <i>Microsoft updates bulletin</i> ³⁸	Windows 95/98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 5.01, SP1-SP3, 5.5, SP1-SP2, 6.0, SP1, 6.0 for Windows Server 2003	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'BR549.dll' ActiveX control due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; a Cross-Domain vulnerability exists in the way Internet Explorer retrieves files from the cache, which could let a remote malicious user execute arbitrary scripting in the "My Computer Zone;" and a vulnerability exists because Internet Explorer does not properly determine object types, which could let a remote malicious user execute arbitrary code. <i>V1.1 Bulletin updated to add information regarding ASP.NET related issues with Windows XP patch.</i> <i>V1.2 Bulletin updated to add details to reboot information in Additional Information section.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-032.asp	Internet Explorer Multiple Vulnerabilities CVE Names: CAN-2003-0530, CAN-2003-0531, CAN-2003-0532	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the IE Object Type vulnerability.

³⁵ Microsoft Security Bulletin MS03-020 V1.1, June 4, 2003.

³⁶ SecurityFocus, August 26, 2003.

³⁷ Microsoft Security Bulletin, MS03-032, August 20, 2003.

³⁸ Microsoft Security Bulletin, MS03-032, 1.1 & 1.2 August 25 & 28, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ³⁹	Windows 95/98/ME/NT 4.0/2000, XP	Office 2000, SP2&SP3, Office XP, SP1&SP2, Project 2000, 2002, Visio Professional 2002, Visual Basic for Applications SDK 5.0, SDK 6.0, SDK 6.2, SDK 6.3	A buffer overflow vulnerability exists because VBA does not properly check certain document properties passed to it when a document is opened by the host application, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-037.asp	Visual Basic for Applications (VBA) Remote Buffer Overflow CVE Name: CAN-2003-0347	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁴⁰	Windows	Office 97, 2000, XP, Word 98 (J), FrontPage 2000, 2002, Publisher 2000, 2002, Works Suite 2001, 2002, 2003	A buffer overflow vulnerability exists because the WordPerfect converter does not correctly validate certain parameters when it opens a WordPerfect document, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-036.asp	Microsoft Converter for WordPerfect Remote Buffer Overflow CVE Name: CAN-2003-0666	High	Bug discussed in newsgroups and websites.
Microsoft ⁴¹	Windows XP	Windows XP Home, SP1, XP Media Center Edition, XP Professional, SP1	A vulnerability exists because some SYN packets transmitted may not have correctly zeroed out URG flags, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Windows XP TCP Packet Information Leakage	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ⁴²	Windows 95/98/ME/NT 4.0/2000, XP	Word 2000, SR1a, SR1, SP2&SP3, Word 2002, SP1&SP2, Word 97, SR1&SR2, Word 98, Japanese Version, Works Suite 2001, 2002, 2003	A vulnerability exists because Word does not properly check certain properties in a modified document and it is possible to craft a malicious document that will bypass the macro security model (even if macro security features are enabled), which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-035.asp	Microsoft Word Document Validation Error CVE Name: CAN-2003-0664	High	Bug discussed in newsgroups and websites.

³⁹ Microsoft Security Bulletin, MS03-037, September 3, 2003.

⁴⁰ Microsoft Security Bulletin, MS03-036 V1.1, September 4, 2003.

⁴¹ SecurityFocus, September 2, 2003.

⁴² Microsoft Security Bulletin, MS03-035, September 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁴³	Windows NT 4.0/2000, XP, 2003	Windows 4.0 Terminal Server, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Windows Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP Home, SP1, XP Professional, SP1	An information disclosure vulnerability exists in the NetBIOS Name Service (NBNS) because datagrams are padded with random memory content when replying to Name Service queries, which could let a remote malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-034.asp	Windows NetBIOS Name Service Information Disclosure CVE Name: CAN-2003-0661	Medium	Bug discussed in newsgroups and websites.
Minihttp ⁴⁴	Windows 2000, XP	File Sharing for Net 1.5	A Directory Traversal vulnerability exists due to a failure to parse user-supplied input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	File Sharing for Net Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required however, an exploit has been published.
Multiple Vendors ⁴⁵	Windows 95/98/ME/ NT 4.0/2000, XP	Go2Call Cash Calling; Net2Phone Net2Phone Dialer ; Yahoo! Messenger 4.0, 5.0, 5.0.1232, 5.0.1065, 5.0.1046, 5.5	A remote Denial of Service vulnerability exists in PC2Phone products due to a failure to handle long bogus UDP packets.	No workaround or patch available at time of publishing.	Multiple Vendor PC2Phone Software Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

⁴³ Microsoft Security Bulletin, MS03-034, September 3, 2003.

⁴⁴ SecurityTracker Alert. 1007588, August 28, 2003.

⁴⁵ Bugtraq, September 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁴⁶ <i>Vendors issues updates^{47, 48}</i>	Unix	Linux kernel 2.4.0-test1-2.4.0-test12, 2.4-2.4.17, 2.4.18, 2.4.18 x86, 2.4.18 pre-1-2.4.18 pre-8, 2.4.19, 2.4.19 -pre1-2.4.19 pre6, 2.4.20, 2.4.21, 2.4.21 pre1, 2.4.21 pre4	A remote Denial of Service vulnerability exists in the 'decode_fh' function in 'nfs3xdr.c' due to a failure to handle a negative size value in certain NFS calls.	Debian: http://security.debian.org/pool/updates/main/k Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000730 RedHat: http://www.redhat.com/	Linux Kernel 2.4 'nfsexdr.c' Remote Denial of Service CVE Name: CAN-2003-0619	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Multiple Vendors ^{49, 50, 51, 52}	Unix	pam_smb 1.1-1.1.6, 2.0 -rc4,; RedHat pam_smb-1.1.6-2.i386.rpm, 1.1.6-2.ia64.rpm, 1.1.6-5.i386.rpm, 1.1.6-7.i386.rpm	A buffer overflow vulnerability exists due to a boundary error when handling passwords, which could let a remote malicious user execute arbitrary code with root privileges.	Debian: http://security.debian.org/pool/updates/main/libp/libpam-smb/ RedHat: ftp://updates.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/	Pam_SMB Remote Buffer Overflow CVE Name: CAN-2003-0686	High	Bug discussed in newsgroups and websites. Exploit script has been published.

⁴⁶ Bugtraq, July 29, 2003.

⁴⁷ Conectiva Security Announcement, CLSA-2003:730, September 1, 2003.

⁴⁸ RedHat Security Advisories, RHSA-2003:198-17, RHSA-2003:239-13, August 21, 2003.

⁴⁹ Debian Security Advisory, DSA 374-1, August 26, 2003.

⁵⁰ Red Hat Security Advisories, RHSA-2003:261-01 & RHSA-2003:262-07, August 26, 2003.

⁵¹ Turbo Linux Security Announcement, TLSA-2003-50, August 29, 2003.

⁵² SuSE Security Announcement, SuSE-SA:2003:036, September 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{53, 54, 55, 56}	Unix	Martin K. Peterson gdm 2.4.1, 2.4.1.1-2.4.1.6; RedHat gdm-2.4.0.7-13.i386.rpm, 2.4.1.3-5.i386.rpm	A vulnerability exists in GDM (Gnome Display Manager) 'examine session errors' feature due to insufficient sanity checks, which could let a malicious user obtain sensitive information.	Mandrake: http://www.mandrakesecure.net/en/advisories/ RedHat: ftp://updates.redhat.com/ Slackware: ftp://ftp.slackware.com/ SOT Linux: ftp://ftp.sot.com/updates/2003/ TurboLinux: http://www.turbolinux.com/update	GDM Xsession-Errors CVE Name: CAN-2003-0547	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors ^{57, 58,} <i>RedHat issues another advisory⁵⁹</i> <i>Conectiva issues advisory⁶⁰</i>	Unix	Linux kernel 2.4.0-test1-test12, 2.4-2.4.20	A remote Denial of Service vulnerability exists because some types of network traffic are not properly handled.	Debian: http://security.debian.org/pool/updates/main/k/ RedHat: ftp://updates.redhat.com/ Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000730	Linux Kernel Excessive Traffic Remote Denial of Service CVE Name: CAN-2003-0364	Low	Bug discussed in newsgroups and websites.

⁵³ Mandrake Linux Security Update Advisory, MDKSA-2003:085, August 21, 2003.

⁵⁴ Red Hat Security Advisory, RHSA-2003:258-01, August 21, 2003.

⁵⁵ SOT Linux Security Advisory, SLSA-2003:37, August 26, 2003.

⁵⁶ Turbolinux Security Announcement, TLSA-2003-08-27, August 27, 2003.

⁵⁷ Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.

⁵⁸ Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.

⁵⁹ Red Hat Security Advisory, RHSA-2003:195-06, June 19, 2003.

⁶⁰ Conectiva Linux Announcement, CLSA-2003:730, September 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 61, 62, 63</p> <p><i>Hewlett Packard issues another advisory</i>⁶⁴</p>	Windows, OpenVMS, Unix	<p>Compaq OpenVMS 7.1 Alpha, 7.1 -2 Alpha, 7.1 VAX, 7.2 -2 Alpha, 7.2 -1H2 Alpha, 7.2 -1H1 Alpha, 7.2 VAX, 7.2 Alpha, 7.2.1 Alpha, 7.3 VAX, Alpha, Tru64 5.0 a, 5.1 a, 5.1;</p> <p>Cray UNICOS 6.0 E, 6.0, 6.1, 7.0, 8.0, 8.3, 9.0, 9.0.2.5, 9.2.4 , 9.2, UNICOS MAX 1.3.5, 1.3, UNICOS/ mk 1.5, 1.5.1, 2.0.5.54;</p> <p>Entegrity DCE/DFS for Linux 2.1, DCE/DFS for Tru64 Unix 4.1.6, 4.2.2, PC-DCE for Windows 4.0.8, 5.0.1; HP HP-UX 10.20, 11.0; IBM DCE 2.2 for Windows, 3.1 for Solaris, AIX, 3.2 for Solaris, AIX</p>	A remote Denial of Service vulnerability exists in multiple vendor OSF DCE (Distributed Computer Environment) implementations.	<p><u>Entegrity:</u> http://support.entegrity.com/private/patches/dce/rpcattacks.shtml</p> <p><u>Hewlett Packard:</u> http://itrc.hp.com Patch PHSS_19739, Patch PHSS_17810</p> <p><u>IBM:</u> ftp://ftp.software.ibm.com/software/network/dce/support/ifixes/</p>	Multiple Vendor OSF Distributed Computing Environment Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

⁶¹ CERT/CC Vulnerability Note, VU#377804, August 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 65, 66, 67, 68 <i>More updates issued</i> ^{69, 70}	Unix	CGI.pm 2.73-2.79, 2.93, 2.751, 2.753; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Mandrake Soft Corporate Server 2.1, 8.2, ppc, 9.0, 9.1, ppc, Single Network Firewall 7.2; OpenPKG Current, 1.2, 1.3	A Cross-Site Scripting vulnerability exists in the 'start_form()' function (or other functions that use this function) due to insufficient sanitization of user-supplied HTML and script, which could let a remote malicious user execute arbitrary code.	<u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/ <u>Debian:</u> http://security.debian.org/pool/updates/main/perl/ <u>Mandrake:</u> http://www.mandrakesecure.net/en/ftp.php <u>OpenPKG:</u> http://pgp.openpkg.org <u>TurboLinux:</u> http://www.turbolinux.com/update <u>SOT Linux:</u> ftp://ftp.sot.com/updates/2003	Multiple Vendor CGI.pm 'Start_Form' Cross-Site Scripting CVE Name: CAN-2003-0615	High	Bug discussed in newsgroups and websites. There is no exploit code required.

⁶² Hewlett-Packard Company Security Bulletin, HPSBUX0308-273, August 13, 2003.

⁶³ Hewlett-Packard Company Software Security Response Team, SSRT3608, August 15, 2003.

⁶⁴ Hewlett-Packard Company Security Bulletins, HPSBUX0308-274 & HPSBUX0309-276, August 26, Sept 2, 2003.

⁶⁵ Conectiva Linux Security Announcement, CLA-2003:713, July 29, 2003.

⁶⁶ OpenPKG Security Advisory, OpenPKG-SA-2003.036, August 6, 2003.

⁶⁷ Debian Security Advisory, DSA 371-1, August 12, 2003.

⁶⁸ Mandrake Linux Security Update Advisory, MDKSA-2003:084, August 20, 2003.

⁶⁹ Turbolinux Security Announcement, TLSA-2003-08-27, August 27, 2003.

⁷⁰ SOT Linux Security Advisory, SLSA-2003:38, August 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 71, 72, 73, 74, 75, 76, 77, 78</p> <p><i>More advisories issued⁷⁹, 80, 81</i></p> <p><i>HP releases updates⁸²</i></p>	MasOS X, Unix	<p>FreeBSD 4.0, alpha, 4.0.x, 4.1, 4.1.1, Stable, Release, 4.2, Release, Stable, Stablepre0 50201, pre122300, 4.3, Release, Releng, Stable, 4.4, Releng, Stable, 4.5, Release, Stable, 4.5 Stablepre2 002-03-07, 4.6, Release, Stable, 4.6.2, 4.7, Release, Stable, 4.8, PreRelease 5.0, alpha; NetBSD 1.5-1.5.3, 1.6, 1.6.1; OpenBSD 2.0-2.9, 3.0-3.3; RedHat wu-ftp-2.6.1-16.i386.rpm, 16.ppc.rpm, 18.i386.rpm, 18.ia64.rpm, -2.6.2-5.i386.rpm, 8.i386.rpm Washington University wu-ftp-2.5.0, 2.6.0-2.6.3</p>	A buffer overflow vulnerability exists due to an off-by-one error in the 'fb_realpath()' function when calculating the length of a concatenated string, which could let a remote malicious user obtain root privileges.	<p><u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/</p> <p><u>Debian:</u> http://security.debian.org/pool/updates/main/w/wu-ftpd/</p> <p><u>FreeBSD:</u> ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:08/realpath.patch</p> <p><u>Mandrake:</u> http://www.mandrakesecure.net/en/ftp.php</p> <p><u>NetBSD:</u> ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2003-011-realpath.patch</p> <p><u>OpenBSD:</u> ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/</p> <p><u>RedHat:</u> ftp://updates.redhat.com/</p> <p><u>SuSE:</u> ftp://ftp.suse.com/pub/use</p> <p><u>Apple:</u> http://docs.info.apple.com/article.html?artnum=61798</p> <p><u>Immunix:</u> http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/wu-ftp-2.6.1-6_imnx_8.i386.rpm</p> <p><u>Sun:</u> http://sunsolve.sun.com/patches/linux/security.html</p> <p><u>Hewlett Packard:</u> ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/</p>	<p>Multiple Vendor realpath() Off-By-One Buffer Overflow</p> <p>CVE Name: CAN-2003-0466</p>	High	<p>Bug discussed in newsgroups and websites. Exploit scripts have been published.</p> <p><i>Another exploit script has been published.</i></p>

⁷¹ Debian Security Advisory, 357-1, July 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{83, 84, 85}	Unix	Martin K. Peterson gdm 2.2.0, 2.2.2.1, 2.2.5 4, 2.4.1, 2.4.1.1- 2.4.1.6; RedHat Enterprise Linux WS 2.1 IA64, 2.1, Linux ES 2.1 IA64, 2.1, Linux AS 2.1 IA64, 2.1, gdm- 2.0beta2- 45.i386. rpm, ppc. rpm, 2.0beta2- 45.ppc. rpm, 2.2.3.1- 20.i386. rpm, 20.ia64. rpm, gdm- 2.2.3.1- 22.i386. rpm, gdm- 2.4.0.7- 13.i386. rpm, gdm- 2.4.1.3- 5.i386.rpm, Linux Advanced Work Station 2.1	Multiple remote Denial of Service vulnerabilities exist when X Display Manager Control XDMCP is running in conjunction with GDM.	Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/advisories/ RedHat: ftp://updates.redhat.com/	Multiple XDMCP GDM Multiple Remote Denial of Service Vulnerabilities CVE Names: CAN-2003-0548, CAN-2003-0549	Low	Bug discussed in newsgroups and websites.

⁷² Mandrake Linux Security Update Advisory, MDKSA-2003:080, July 31, 2003.

⁷³ Red Hat Security Advisory, RHSA-2003:245-01, July 31, 2003.

⁷⁴ SuSE Security Announcement, SuSE-SA:2003:032, July 31, 2003.

⁷⁵ Conectiva Linux Security Announcement, CLA-2003:715, August 1, 2003.

⁷⁶ FreeBSD Security Advisory, FreeBSD-SA-03:08, August 4, 2003.

⁷⁷ NetBSD Security Advisory 2003-01, August 4, 2003.

⁷⁸ Turbolinux Security Advisory, TLSA-2003-46, August 4, 2003.

⁷⁹ Immunix Secured OS Security Advisory, IMNX-2003-7+-019-01, August 7, 2003.

⁸⁰ Apple Security Update, 61798, August 14, 2003.

⁸¹ Sun Advisory, August 18, 2003.

⁸² Hewlett-Packard Company Security Bulletin, HPSBUX0309-277, September 2, 2003.

⁸³ Mandrake Linux Security Update Advisory, MDKSA-2003:085, August 21, 2003.

⁸⁴ Red Hat Security Advisories, RHSA-2003:258-01 & RHSA-2003:259-07, August 21, 2003.

⁸⁵ Conectiva Linux Security Announcement, CLA-2003:729, August 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{86, 87, 88, 89, 90, 91, 92, 93, 94}	MacOS X 10.2x nix	FreeBSD 4.6-4.8, 5.0; OpenBSD 3.2; RedHat sendmail-8.12.5-7.i386.rpm, 8.12.8-4.i386.rpm, cf-8.12.5-7.i386.rpm, cf-8.12.8-4.i386.rpm, devel-8.12.5-7.i386.rpm, devel-8.12.8-4.i386.rpm, doc-8.12.5-7.i386.rpm, oc-8.12.8-4.i386.rpm; Sendmail Consortium Sendmail 8.12.1-8.12.8; SGI IRIX 6.5.19-.5.21	A vulnerability exists when implementing the use of DNS Maps due to a failure to properly initialize dynamically allocated data, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	SendMail Consortium: ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.9.tar.gz Conectiva: ftp://atualizacoes.conectiva.com.br/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:11/sendmail_patch Hewlett Packard: http://www.securityfocus.com/advisories/5774 Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.2/common/016_sendmail_patch OpenPKG: ftp.openpkg.org RedHat: ftp://updates.redhat.com/ SGI: ftp://patches.sgi.com/support/free/security/patches/ SOT Linux: ftp://ftp.sot.com/updates/2003/ SuSE: ftp://ftp.suse.com/pub/suse/i386/update/	Sendmail DNS Maps Remote Denial of Service CVE Name: CAN-2003-0688	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Netbula LLC ⁹⁵	Windows, Unix	Anyboard 9.9.5 6	An information disclosure vulnerability exists in the 'anyboard.cgi' script when a specially crafted HTTP request is submitted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Anyboard Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁸⁶ SGI Security Advisory, 20030803-01-P, August 25, 2003.

⁸⁷ FreeBSD Security Advisory, FreeBSD-SA-03:11, August 26, 2003.

⁸⁸ SuSE Security Announcement, SUSE-SA:2003:035, August 26, 2003.

⁸⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:086, August 26, 2003.

⁹⁰ OpenPKG Security Advisory, OpenPKG-SA-2003.037, August 28, 2003.

⁹¹ Red Hat Security Advisory, RHSA-2003:265-01, August 28, 2003.

⁹² Conectiva Linux Security Announcement, CLA-2003:727, August 29, 2003.

⁹³ SOT Linux Security Advisory, SLSA-2003:39, August 29, 2003.

⁹⁴ Hewlett-Packard Security Advisory, SSRT3612, September 5, 2003.

⁹⁵ Secunia Security Advisory, August 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetWin ⁹⁶ <i>Upgrade now available</i> ⁹⁷	Windows NT 4.0/2000, XP, 2003, Unix	Surge LDAP 10.0d	Multiple vulnerabilities exist: a path disclosure vulnerability exists in the web server component when a HTTP GET request is issued for an invalid resource, which could let a remote malicious user obtain sensitive information; a remote Denial of Service vulnerability exists when a long URL is requested; a vulnerability exists in 'surgeldap\user.dat' because usernames and passwords are stored in plaintext, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in the 'user.cgi' script due to insufficient verification of the 'cmd' parameter, which could let a remote malicious user execute arbitrary code.	<i>Upgrade available at:</i> http://netwinsite.com/surgeldap/updates.htm	SurgeLDAP Multiple Vulnerabilities	Low/Medium/High (Low if a DoS; Medium is sensitive information can be obtained; and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required however, an exploit has been published. Denial of Service vulnerability may be exploited via a web browser.
newsPHP Development Team ⁹⁸	Windows, Unix	newsPHP 216	Two vulnerabilities exist: a vulnerability exists in the 'nphpd.php' module because the language file parameter isn't properly verified if it is undefined in the configuration file, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to improper verification of authentication credentials, which could let a remote malicious user obtain sensitive information or perform unauthorized actions.	No workaround or patch available at time of publishing.	newsPHP 'nphpd.php' Module & Authentication Bypass	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

⁹⁶ Securiteam, August 14, 2003.

⁹⁷ SecurityFocus, September 1, 2003.

⁹⁸ Securiteam, August 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell ⁹⁹	Multiple	iChain Server 2.2, SP1, FP1a, FP1	A Denial of Service vulnerability exists when a retrieve request is submitted by 'wget' on a directory that has no files.	Workaround: Create a dummy file (small text file) in each of the following directories: sys:\etc\proxy\appliance\config\user\cert\backup\ sys:\etc\proxy\appliance\config\user\cert\temp\ sys:\etc\proxy\appliance\config\user\cert\ics\ sys:\etc\proxy\appliance\config\user\cert\sc\ sys:\etc\proxy\appliance\config\user\cert\tr\	iChain Denial of Service	Low	Bug discussed in newsgroups and websites.
OpenBSD ¹⁰⁰	Unix	OpenBSD 3.3	A Denial of Service vulnerability exists in the semget() system call due to insufficient bounds checking.	Upgrade available at: http://www.openbsd.org/errata.html	OpenBSD semget() Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
OptiSoft ¹⁰¹	Windows	Blubster 2.5	A remote Denial of Service vulnerability exists when a malicious user floods port 701 with voice chat session requests.	No workaround or patch available at time of publishing.	Blubster Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Padl Software ¹⁰²	Unix	pam_ldap Build 161	A vulnerability exists due to an error in 'pam_filter,' which could let a remote malicious user bypass certain host-based access restrictions.	Upgrade available at: http://www.padl.com/download/pam_ldap.tgz Mandrake: http://www.mandrakesecure.net/en/ftp.php	PAM_LDAP PAM Filter Access Restriction Failure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
phpGACL ¹⁰³	Windows, Unix	phpGACL 3.0.2, 3.1.0b4, 3.1.0b3, 3.1.0b2, 3.1.0b, 3.1.0, 3.1.1b3, 3.1.1 b2, 3.1.1	A vulnerability exists when '?debug=1' is added to the URL, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://prdownloads.sourceforge.net/phpgac1/3.2.0b.tar.gz?download	PHPGACL Debugging Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

⁹⁹ Novell Technical Document, 10086051, August 20, 2003

¹⁰⁰ SecurityTracker Alert, 1007543, August 20, 2003.

¹⁰¹ Securiteam, August 24, 2003.

¹⁰² Mandrake Linux Security Update Advisory, MDKSA-2003:088, September 3, 2003.

¹⁰³ SecurityFocus, August 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Pierre-Yves Legendre ¹⁰⁴	Windows, Unix	Py-Membres 4.0-4.2	Several vulnerabilities exist: an input validation vulnerability exists in the 'pass_done.php' script, which could let a remote malicious user execute arbitrary SQL commands; and a vulnerability exists in the 'admin/secure.php' script due to insufficient verification, which could let a remote malicious user obtain administrator access.	No workaround or patch available at time of publishing.	Py-Membres Secure.PHP Unauthorized Access	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Piolet Networks ¹⁰⁵	Windows	Piolet 1.0.5	A remote Denial of Service vulnerability exists due to a failure to handle a large number of requests on port 701/tcp.	No workaround or patch available at time of publishing.	Piolet Client Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Polycom ¹⁰⁶ <i>Fix should be available</i> ¹⁰⁷	Multiple	MGC-100, MGC-25 5.51.21, 5.51.211, MGC-50	A remote Denial of Service vulnerability exists in the administrative interface when multiple packets are submitted to the service (port 5003/tcp).	<i>The vendor has announced that the fix will be available on August 26. Users are advised to contact support to obtain it.</i>	Polycom MGC Systems Remote Administration Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with one of several freely available utilities.
Real Networks ¹⁰⁸ <i>Proof of Concept exploit published</i> ¹⁰⁹	Windows 95/98/ME/NT 4.0/2000, XP	RealOne Desktop Manager, RealOne Enterprise Desktop 6.0.11.774, RealOne Player 6.0.11.853, 6.0.11.841, 6.0.11.830, 6.0.11.818, 2.0, RealOne Player Gold for Windows 6.0.10 .505	A vulnerability exists due to an unspecified error in the handling of SMIL files, which could let a remote malicious user execute arbitrary code.	Updates available at: http://www.service.real.com/help/faq/security/securityupdate_august2003.html	RealOne Player SMIL File Script Execution	High	Bug discussed in newsgroups and websites. <i>Proof of Concept exploit has been published.</i>

¹⁰⁴ SecurityTracker Alert, 1007581, August 26, 2003.

¹⁰⁵ Bugtraq, August 20, 2003.

¹⁰⁶ Exploitlabs.com Advisory, EXPL-A-2003-014, July 12, 2003.

¹⁰⁷ SecurityFocus, August 23, 2003.

¹⁰⁸ RealNetworks Security Advisory, August 19, 2003.

¹⁰⁹ SecurityFocus, August 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Real Networks ¹¹⁰	Windows NT 4.0/2000, XP, Unix	Helix Universal Server 8.01, 9.01, 9.0, Real Server 7.0, 7.0.1, 7.0.2, 8.0 Beta, 8.0, 8.01, 8.02, G21.0	A buffer overflow vulnerability exists because the 'vsreplin.so' and 'vsreplin.dll' plugins fail to handle long requests, which could let a remote malicious user execute arbitrary code with root privileges.	Workaround available at: http://www.service.real.com/help/faq/security/rootexploit082203.html	Helix Universal Server Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Real Networks ¹¹¹ <i>Exploit has been published</i> ¹¹²	Windows 95/98/ME/NT 4.0/2000, XP	RealOne Desktop Manager, RealOne Enterprise Desktop 6.0.11.774, RealOne Player 6.0.11.853, 6.0.11.841, 6.0.11.830, 6.0.11.818, 2.0, RealOne Player Gold for Windows 6.0.10 .505	A vulnerability exists due to an unspecified error in the handling of SMIL files, which could let a remote malicious user execute arbitrary code.	Updates available at: http://www.service.real.com/help/faq/security/securityupdate_august2003.html	RealOne Player SMIL File Script Execution	High	Bug discussed in newsgroups and websites. <i>Exploit has been published.</i>
RedHat ¹¹³	Unix	Enterprise Linux WS 2.1 IA64, 2.1, ES 2.1 IA64, 2.1, AS 2.1 IA64, 2.1	A buffer overflow vulnerability exists in the 'getgrouplist' function if the size of the group list is too small to hold all the user's groups, which could let a malicious user cause a Denial of Service.	Patches available at: http://rhn.redhat.com/errata/RHSA-2003-249.html	Glibc Getgrouplist Function Buffer Overflow CVE Name: CAN-2003-0689	Low	Bug discussed in newsgroups and websites.
RedHat ¹¹⁴	Unix	Enterprise Linux WS 2.1 IA64, ES 2.1 IA64, AS 2.1 IA64	A race condition vulnerability exists in the 'malloc' function in the glibc library, which could let a malicious user corrupt memory.	Patches available at: http://rhn.redhat.com/errata/RHSA-2003-249.html	Glibc Malloc Routine Race Condition	Medium	Bug discussed in newsgroups and websites.

¹¹⁰ Securiteam, August 26, 2003.

¹¹¹ RealNetworks Security Advisory, August 19, 2003.

¹¹² SecurityFocus, August, 27, 2003.

¹¹³ RedHat Security Advisory, RHSA-2003:249-11, August 22, 2003.

¹¹⁴ RedHat Security Advisory, RHSA-2003:249-11, August 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat ¹¹⁵	Unix	iptables-1.2.1a-1.i386.rpm, iptables-1.2.3-1.i386.rpm, iptables-1.2.5-3.i386.rpm, iptables-1.2.6a-2.i386.rpm, iptables-ipv6-1.2.1a-1.i386.rpm, iptables-ipv6-1.2.3-1.i386.rpm, iptables-ipv6-1.2.5-3.i386.rpm, iptables-ipv6-1.2.6a-2.i386.rpm	A vulnerability exists because recent updates to the kernel did not also update the iptables utility, which may prevent the iptables firewall from functioning correctly.	Updates available at: ftp://updates.redhat.com/	RedHat Linux IPTables Firewall Failure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Regents of University of California ¹¹⁶	Unix	bsd-games 2.9, 2.12-2.14	A buffer overflow vulnerability exists in 'Monop' due to insufficient bounds checking of player names, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	BSD-Games Monop Player Name Buffer Overrun	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Sand-sprite.com ¹¹⁷ <i>Vendor response</i> ¹¹⁸	Windows	Web Chat Server	An input validation vulnerability exists which could let a remote malicious user execute arbitrary HTML and script code.	<i>Vendor Response: Chatserver is a skeleton application designed to teach the concept of http chunked transfers to developers. It is not designed for, or capable of production use. Its own readme states the same concerns declared in this advisory. There will be no patch released because such is outside of the applications design intent. Please refer to the applications Readme file for more details.</i>	Web ChatServer Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

¹¹⁵ RedHat Security Advisory, RHSA-2003:213-01, August 25, 2003.

¹¹⁶ Securiteam, August 26, 2003.

¹¹⁷ Exploitlabs Advisory, EXPL-A-2003-019, August 9, 2003.

¹¹⁸ SecurityFocus, August 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SAP ¹¹⁹	Windows	Internet Transaction Server 4620.2.0.32 3011 Build 46B. 323011	Several vulnerabilities exist: a information disclosure vulnerability exists when malformed requests are handled, which could let a remote malicious user obtain sensitive information; a Directory Traversal vulnerability exists due to a failure to parse user-supplied input, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in the 'wgate.dll' component due to insufficient sanitization of data supplied to the 'wgate.dll' library, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SAP Internet Transaction Server Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit has been published for the information disclosure vulnerability and a Proof of Concept exploit has been published for the Directory Traversal & Cross-Site Scripting vulnerabilities.
SCO ¹²⁰	Unix	Caldera OpenLinux Server 3.1.1, Workstation 3.1.1, OpenServer 5.0.7; SCO Unixware 7.1.3	A vulnerability exists because Docview configures the Apache web server in a way that allows remote malicious users to read arbitrary publicly readable files via a certain URL, possibly related to rewrite rules.	Upgrades available at: ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/ ftp://ftp.caldera.com/pub/updates/OpenServer/CSSA-2003-SCO.16/ ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.18/	DocView File Disclosure CVE Name: CAN-2003-0658	Medium	Bug discussed in newsgroups and websites.
Site-builder ¹²¹	Windows, Unix	EZ-Web Sitebuilder 1.4	A Directory Traversal vulnerability exists in the 'sitebuilder.cgi' script due to a failure to parse user-supplied input, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Sitebuilder 'sitebuilder.cgi' Directory Traversal File Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
SLRN Development Team ¹²²	Unix	slrn 0.9.6.4, 0.9.6.3, 0.9.6.2-9, 0.9.6.2, 0.9.7.0-0.9.7.4	A buffer overflow vulnerability exists when handling malicious 'XRef' headers, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=7768	SLRN XRef Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.

¹¹⁹ SEC-CONSULT Security Report, August 30, 2003.

¹²⁰ SCO Security Advisories, CSSA-2003-SCO.16, CSSA-2003-SCO.18, & CSSA-2003-021.0, August 22 &25, 2003.

¹²¹ SecurityFocus, September 1, 2003.

¹²² SecurityFocus, August 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Srcpd ¹²³	Unix	Srcpd 2.0	Several vulnerabilities exist in the 'srcpd' Simple Railroad Command Protocol daemon: an integer overflow vulnerability exists which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; and several buffer overflow vulnerabilities exist in the handleSET(), handleGET(), and other method handlers due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Srcpd Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the Denial of Service vulnerability. Exploit script has been published for the buffer overflow vulnerabilities.
Sun Microsystems, Inc. ¹²⁴	Unix	Solaris2.6, 2.6_x86, 7.0, 7.0_x86	A vulnerability exists because some patches designed to fix 'cachefs' vulnerabilities may cause various sections of the local inetd.conf file to be overwritten.	Patches and workaround available at: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert%2F56300&zone_32=category%3Asecurity	Solaris Cachefs Patch Weakness	Medium	Bug discussed in newsgroups and websites.
Tellurian ¹²⁵	Windows 9x, NT 4.0	TftpdNT 1.8, 2.0	A buffer overflow vulnerability exists due to insufficient bounds checking when handling user-supplied filenames, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.tellurian.com.au/products/trinkets/tftpdNT/	TftpdNT Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Tomi Manninen ¹²⁶	Unix	LinuxNode 0.3	Several buffer overflow vulnerabilities exist due to a boundary error in the 'expand_string()' function as well as some format string errors due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code and obtain root privileges.	Update available at: http://hes.iki.fi/pub/ham/unix/linux/ax25/ Debian: http://security.debian.org/pool/updates/main/n/node/	LinuxNode Remote Buffer Overflows	High	Bug discussed in newsgroups and websites.
TSguest-book ¹²⁷	Windows, Unix	TSguest-book 2.1	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML from user-supplied input in the 'message' variable, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	TSguestbook Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required, however, a Proof of Concept exploit has been published.

¹²³ m00 security advisory #001, August 21, 2003.

¹²⁴ Sun(sm) Alert Notification, 56300, August 20, 2003.

¹²⁵ Securiteam, August 26, 2003.

¹²⁶ Debian Security Advisory, DSA 274-1, August 29, 2003.

¹²⁷ Zone-h Security Team Advisory, ZH2003-26SA, September 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
University of Cambridge ¹²⁸	Unix	Exim 3.0, 3.3, 3.3 1, 3.3 2, 3.11-3.22, 3.30-3.36, 4.10, 4.20	A buffer overflow vulnerability exists due to insufficient bounds checking when handling user-supplied 'SMTP EHLO/HELO' data, which could let a remote malicious user execute arbitrary code.	Updates available at: http://www.exim.org/mirrors.html Patches available at: http://www.exim.org/pipermail/exim-users/Week-of-Mon-20030811/057720.html Debian: http://security.debian.org/pool/updates/main/e/exim/	Exim EHLO/HELO Remote Buffer Overflow CVE Name: CAN-2003-0698	High	Bug discussed in newsgroups and websites.
vpop3d ¹²⁹	Unix	vpop3d	A local/remote Denial of Service vulnerability exists due to insufficient handling of excessive length USER name values.	No workaround or patch available at time of publishing.	Vpop3d Local/Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
wap-serv.com ¹³⁰	Windows 98/NT 4.0/2000	WapServ Enterprise 1.0, Lite 1.0, Pro 1.0	Multiple remote Denial of Service vulnerabilities exist when malicious data is received and processed over ports 9200 and 9201.	No workaround or patch available at time of publishing.	WapServ Multiple Remote Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
World Flash ¹³¹	Multiple	News Ticker Gold M5.30i	A buffer overflow vulnerability exists when HTML data is received from remote sites due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	News Ticker Remote Buffer Overrun	High	Bug discussed in newsgroups and websites.
XFree86 ¹³²	Unix	XFree86 X11R6 4.3	Multiple vulnerabilities exist due to integer overflows that may occur in the transfer and enumeration of fonts from font servers to clients, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	XFree86 Font Library Integer Overflows	High	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

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.

¹²⁸ Debian Security Advisory, DSA 376-1, September 4, 2003.

¹²⁹ Bugtraq, August 22, 2003.

¹³⁰ SecurityTracker Alert ID, 1007555, August 22, 2003.

¹³¹ Bugtraq, August 28, 2003.

¹³² Securiteam, September 2, 2003.

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.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between August 20 and September 2, 2003, listed by date of script, script names, script description, and comments. 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. During this period, 23 scripts, programs, and net-news messages containing holes or exploits were identified. *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
September 2, 2003	getints.c	Script that exploits the Firewall-1 SecuRemote Information Leakage vulnerability.
September 2, 2003	linux_pam_smb.c	Script that exploits the Pam_SMB Remote Buffer Overflow vulnerability.
August 29, 2003	atakemul.c	Script that exploits the eMule Denial of Service vulnerability.
August 29, 2003	messmule.c	Script that exploits the eMule 'OP_SERVERMESSAGE' Format String vulnerability.
August 29, 2003	Wellenreiter-v1.9.tar.gz	A GTK/Perl wireless network discovery and auditing tool. Its scanner window can be used to discover access-points, networks, and ad-hoc cards and also detects essid broadcasting or non-broadcasting networks, WEP capabilities, and the manufacturer automatically.
August 28, 2003	xgkftpd.c	Script that exploits the GTKFTPD LIST Command Remote Buffer Overflow vulnerability.
August 27, 2003	0wn-smpc.pl	Perl script that exploits the SNMPc v5/v6 Unauthorized Remote Privileged Access vulnerability.
August 26, 2003	fm-IE.tar	Perl script that exploits the Microsoft Internet Explorer OBJECT Tag Buffer Overflow vulnerability.
August 26, 2003	tftp-bof.pl	Perl script that exploits the TftpdNT Remote Buffer Overflow vulnerability.
August 26, 2003	kismet-3.0.1.tar.gz	A 11b wireless network sniffer that is capable of sniffing using almost any wireless card supported in Linux, which currently divide into cards handled by libpcap and the Linux-Wireless extensions (such as Cisco Aironet), and cards supported by the Wlan-NG project which use the Prism/2 chipset (such as Linksys, Dlink, and Zoom).
August 25, 2003	monosex.c	Script that exploits the BSD-Games Monop Player Name Buffer Overrun vulnerability.
August 25, 2003	THCREALbad.zip	Exploit for the Helix Universal Server Remote Buffer Overflow vulnerability.
August 25, 2003	THCREALbad.c	Exploit for the Helix Universal Server Remote Buffer Overflow vulnerability.
August 25, 2003	DSR-virobot.pl	Perl script that exploits the ViRobot Linux Server Buffer Overflows vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
August 25, 2003	frontkey.tgz	Remote administration kernel module designed for the 2.4 series that replaces system calls by inserting a push ret at the beginning of system_call, making the program jump to specified code. It provides a remote terminal backdoor through SYS_read hooking which means you can enter the box through any open tcp port.
August 25, 2003	intersystems2.txt	Further information, research, and exploits in regards to the InterSystems Cache vulnerabilities.
August 25, 2003	dnsenum.zip	A Perl script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results.
August 25, 2003	intrusion-agent.pdf	White paper discussing methodologies for accessing internal networks using HTTP tunneling and tricking end users.
August 25, 2003	lkl-0.1.0.tar.gz	A userspace keylogger that runs under Linux x86/arch and logs everything which passes through the hardware keyboard port (0x60).
August 24, 2003	Blubster_Dos.c	Script that exploits the Blubster Remote Denial of Service vulnerability.
August 22, 2003	vpop3dos.pl	Perl script that exploits the Vpop3d Local/Remote Denial of Service vulnerability.
August 21, 2003	m00-srcpd.c	Script that exploits the Srcpd Buffer Overflow vulnerabilities.
August 20, 2003	Piolet_DoS.c	Script that exploits the Piolet Client Remote Denial of Service vulnerability.

Trends

- The CERT/CC has noticed an increase in traffic directed at port 554/tcp. This port is used by the Real Time Streaming Protocol (RTSP). This activity may be related to a recently discovered vulnerability in Real Networks' Media Server. For more information see "Helix Universal Server Remote Buffer Overflow" entry in the "Bugs, Holes & Patches" Table.
- A new worm that exploits the same security weakness as the Blaster worm (also known as "lovsan" or "msblast") has been released on the Internet. This new worm, dubbed "nachi," "welchia," or "msblast.d" does not infect systems that have been updated to counter the Blaster worm in accordance with Microsoft's instructions <http://www.microsoft.com/security/incident/blast.asp>. This new worm will re-infect computers that are currently infected with Blaster or one of its variants. It deletes the original worm, patches the system by downloading the update from Microsoft, and replaces the original worm with itself. For more information see Department of Homeland Security advisory located at: <http://www.nipc.gov/warnings/advisories/2003/Advisory8182003.htm>
- **The DHS/Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSA) has issued a second update to the security advisory on Microsoft's DCOM RPC Buffer Overflow vulnerability. Malicious code dubbed "MSBLAST," "LOVSAN," or "BLASTER" began circulating on the Internet on August 11th. This worm takes advantage of the vulnerability discussed in Microsoft's advisory located at: <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp> and contains code that will target Microsoft's update servers on August 16th. This additional attack could cause significant Internet-wide disruptions. It is also possible that other worms based on this vulnerability will be released over the next few days as "copy cat" attacks. Also numerous exploits and Trojans have been reported in the wild that exploit this vulnerability. Please ensure that you have applied the Microsoft patch for this vulnerability.**

- Online vandals are using a program to compromise Windows servers and remotely control them through Internet relay chat (IRC) networks. Several programs, including one that exploits a recent vulnerability in computers running Windows, have been cobbled together to create a remote attack tool. The tool takes commands from an attacker through the IRC networks and can scan for and compromise computers vulnerable to the recently discovered flaw in Windows
- The CERT/CC has received reports of systems being compromised by two recently discovered vulnerabilities in the Microsoft Remote Procedure Call (RPC) service. Additionally, the CERT/CC has received reports of widespread scanning for systems with open Microsoft RPC ports (135, 139, 445). For more information, see “Exploitation of Microsoft RPC Vulnerabilities” located at: <http://www.cert.org/current/>.
- The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSA) has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting a vulnerability in popular Microsoft Windows operating systems. DHS expects that exploits are being developed for malicious use. For more information see, “Bugs, Holes & Patches” Table “Windows DCOM RPC Buffer Overflow” and DHS/IAIP Advisory located: <http://www.nipc.gov/warnings/advisories/2003/Potential72403.htm>. Additional information on the Microsoft vulnerability may also be found at: <http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>.
- Recent reports to the CERT/CC have highlighted two chronic problems:
 - The speed at which viruses are spreading is increasing. This echoes the trend toward faster propagation rates seen in the past few years in self-propagating malicious code (i.e., worms). A similar trend from weeks to hours has emerged in the virus (i.e., non-self-propagating malicious code) arena.
 - In a number of the reports, users who were compromised may have been under the incorrect impression that merely having antivirus software installed was enough to protect them from all malicious code attacks. This is simply a mistaken assumption, and users must always exercise caution when handling e-mail attachments or other code or data from untrustworthy sources. For more information see, CERT® Incident Note IN-2003-01, located at: http://www.cert.org/incident_notes/IN-2003-01.html.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT.Disom.Worm (Alias: BAT/Disom) (Batch File Worm): This worm spreads through file-sharing networks and IRC. It has a destructive payload that attempts to delete numerous files, including those belonging to some antivirus programs.

MPB/Kynel (Aliases: MBA.First, MpB.Kynel.A, MPB_KYNEL.A) (MapInfo Virus): This is the first known virus to infect MapInfo Tables (an element of the MapInfo Professional product for Windows). Systems that do not run the MapInfo product are not at risk of getting infected by this virus. This virus functions in a similar manner to Excel macro viruses, in that it drops a file containing executable code into an application "startup folder" and after this event each newly created/modified workspace becomes infected. MapInfo however requires that a loader, or pointer, file, STARTUP.WOR, is used to call this dropped executable file; in this case 0gPiSs1.dll (a MapBasic executable).

Raleka.C (Aliases: Worm.Win32.Raleka.C, W32/Raleka.C, W32/Raleka.C.worm, WORM_RALEKA.C) (Win32 Worm): Raleka.C is minor variant of the Raleka.A worm. In this variant the update URL has been changed.

VBS/Inor (Visual Basic Script Worm): This detection is for Visual Basic scripts intended to drop and execute other (potentially malicious) files on the victim machine. Multiple versions of this script are known. The script was referenced in spammed HTML formatted e-mails. The script bears similarities to Downloader-BO.dr.

W32.Bigfairy.A@mm (Win32 Worm): This Visual Basic worm tries to send itself to all the contacts in your address book.

W32.Blaster.E.Worm (Aliases: W32/Msblast.E, Lovsan.E, Worm/Lovsan.E, W32/Blaster-E, W32/Lovsan.worm.e, Worm.Win32.Lovsan, WORM_MSBLAST.GEN) (Win32 Worm): This worm exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135. The worm targets only Windows 2000 and Windows XP computers. While Windows NT and Windows 2003 Servers are vulnerable to the aforementioned exploit (if not properly patched), the worm is not coded to replicate to those systems. It attempts to download the Mslaug.exe file into the %Windir%\System32 folder, and then execute it. This worm does not have a mass-mailing functionality, but also attempts to perform a Denial of Service (DoS) on kimble.org.

W32/Blaster-F (Aliases: W32.Blaster.F.Worm, W32/Msblast.F, Lovsan.F, Worm.Win32.Lovsan, W32.Blaster.Worm, WORM_MSBLAST, Worm/Lovsan, W32/Lovsan.worm.f, Win32.Poza.F, WORM_MSBLAST.G) (Win32 Worm): This worm is a functional equivalent to W32/Blaster-A, except for some changes. The worm filename used is enbiei.exe. The registry entry used has been changed to:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\www.hidro.4t.com

The target for the Distributed Denial of Service attack has been changed to tuiasi.ro.

W32/Cailont-B (Alias: W32.Nolor.B@mm) (Win32 Worm): This is an e-mail aware worm. The subject line, message text, and attachment filename of the e-mail are produced by concatenating several randomly chosen phrases. The e-mail contains an HTML component that contains a Visual Basic Script that drops and runs W32/Cailont-B. When run, it copies itself to various folders on the system. The worm will also drop the Visual Basic Script version of itself in one or more files with a DAT extension.

W32/Dumaru.c@MM (Aliases: W32/Dumaru.c@MM, W32/Nugosh-A) (Win32 Worm): This variant of the W32/Dumaru@MM virus contains its own SMTP engine for constructing outgoing messages. The virus arrives in an e-mail message with the following characteristics:

- From: "Microsoft" security@microsoft.com
- Subject: Use this patch immediately !
- Attachment: patch.exe

The worm trawls the harddisk for files with extensions .htm, .wab, .html, .dbx, .tbb, and .abd for e-mail addresses to send itself to. These e-mail addresses are written to file winload.log. The worm contains a keylogger component, which logs user events and key inputs to file vxdload.log, rundllx.sys, or rundlln.sys. From strings within the virus body, it seems that passwords saved in Far Manager, and data from the clipboard are logged as well. Like previous variants, this worm drops the password stealer PWS-Narod.

W32/Gaobot.worm.z (Aliases: W32.HLLW.Gaobot.AA, WORM_AGOBOT.R) (Win32 Worm): This worm attempts to use several vulnerabilities to spread:

- MS03-001 (RPC Locator) MS03-026 (Dcom RPC)

Upon execution, the worm copies itself to %SysDir% as:

- SVCHOS1.EXE
- RPCFIX.EXE (Where %SysDir% is the System directory, for example: C:\WINNT\SYSTEM32.)

The following Registry keys are added to hook system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "MS Config Loader" = SVCHOS1.EXE
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "MS Config Loader" = SVCHOS1.EXE

As for the previous variant, this worm requires MSVCP60.DLL to run - this is a standard MS Visual C DLL, which if not present on the system, would prevent the worm from executing.

W32.HLLW.Astef (Alias: Bloodhound.W32.5) (Win32 Worm): This worm attempts to spread through file-sharing networks, such as KaZaA, KaZaA Lite, Grokster, Bearshare, eDonkey2000, Morpheus, Limewire, Overnet, Papigator, XoloX, Tesla, WinMX, Shareaza, Gnucleus, and ICQ as well.

W32.HLLW.Blaxe (Win32 Worm): This worm attempts to spread itself through the Grokster, KaZaA, and iMesh file-sharing networks. It is written in the Microsoft Visual Basic programming language and is compressed with UPX.

W32.HLLW.Darby (Alias: W32/Bardiel) (Win32 Worm): This worm spreads through file-sharing networks such as KaZaA and Morpheus, and may also attempt to spread through e-mail and IRC. When executed, this worm displays a message box which says either "The file this total or partially damaged, impossible to open the file," or "El archivo esta total o parcialmente danado, imposible abrir el archivo." It is written in Visual Basic and packed with UPX.

W32.HLLW.Deforms.D (Aliases: Worm.Win32.Deform.ac, W32/Deform.worm.gen) (Win32 Worm): This is a worm that attempts to spread through a local network using Windows shares. The worm attempts to connect to TCP ports 139 and 445, through NetBIOS, and does not have a malicious payload.

W32.HLLW.Ihedont@mm (Alias: Bloodhound.W32.VBWORM) (Win32 Worm): This mass-mailing worm replicates by sending itself to the contacts in the Outlook Address Book. It is written in the Microsoft Visual Basic programming language.

W32.HLLW.Lacon@mm (Win32 Worm): This mass-mailing worm attempts to spread itself through e-mail, mIRC, and file-sharing networks. The e-mail has the following characteristics:

- Subject: National No Call Registry Info
- Attachment: No Call List.exe

It is written in the Microsoft Visual Basic (VB) programming language, and the VB run-time libraries must be installed for W32.HLLW.Lacon@mm to run.

W32.Hopalong@mm (Win32 Worm): This mass-mailing worm sends itself to any addresses in the Microsoft Outlook Address Book. The e-mail has the following characteristics:

- Subject: Look At This!!!
- Attachments: hop_along.exe

W32.Kwbot.P.Worm (Aliases: W32/Sdbot.worm.gen, Backdoor.SdBot.gen) (Win32 Worm): This worm attempts to spread through file-sharing networks, such as KaZaA, iMesh, LimeWire, eDonkey2000, and Morpheus. It has backdoor capabilities that allow a malicious user to control a computer by using Internet Relay Chat (IRC). The existence of the file mscommand.exe is an indication of a possible infection. It is compressed with UPX.

W32.Lade (Alias: Backdoor.IRC.Lade) (Win32 Worm): This is a worm that attempts to spread itself through IRC. It attempts to remove antivirus software installed on the host and may attempt to format the hard drive.

W32/Limper (Win32 Worm): When run, this virus infects .EXE files. It deletes the file "Host.EXE" if it exists in the current directory. Infected files will contain the text "[Win32.Limp] [RUiNER /SOS]." The virus body is located at the beginning of the file. The original code has been moved to the end. Running the infected file will directly infect files in the current directory.

W32/Lovgate-P (Win32 Worm): This version of W32/Lovgate-L has been infected with W32/Parite-A and then packed with a compression tool. When the worm is run, the W32/Parite-A component will generate a Windows error. The application or DLL <filename> is not a valid Windows image. The exact error message displayed will vary slightly depending on the version of Microsoft Windows.

W32/Mantibe.worm (Win32 Worm): This detection is for a floppy worm written in MSVB. When run on the victim machine, the worm installs itself into the System directory (with the filename of the executed file). The following Registry key is added to hook system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Mantis" = %SysDir%\filename.exe

It attempts to copy itself to A: with the following filename: BESO.JPG.EXE

W32.Mapson.D.Worm (Win32 Worm): This mass-mailing worm sends itself to all the contacts in the MSN Messenger contact list and also attempts to spread through file-sharing networks and ICQ. It also attempts to terminate some popular antivirus, firewall, and system-monitoring programs. The subject line, message body, and attachment vary, but the attachment will have a .bat, .com, .exe, .scr, .pif, or .txt extension. The worm may also spoof the From: field. It is written in the Borland Delphi programming language and is compressed with UPX.

W32.Neroma@mm (Aliases: W32.Neroma@MM, W32/Neroma@MM, Worm.Win32.Maro.5632) (Win32 Worm): This mass-mailing worm attempts to use Microsoft Outlook to e-mail itself to all the contacts in the Windows Address Book. The e-mail has the following characteristics:

- Subject: It's Near 911!
- Attachment: 911.jpg

It is written in Microsoft Visual Basic (VB) and is UPX-packed.

W32.Pandem.C.Worm (Win32 Worm): This worm attempts to spread by e-mailing itself to contacts in the Microsoft Outlook Address Book, and through file-sharing applications and ICQ. The worm is written in C++ and is packed with PEBundle.

W32/Panoil.c@MM (Win32 Worm): This worm uses Microsoft Outlook to send itself to all the e-mail addresses found in the Outlook Address Book. The e-mail has the following characteristics:

- Subject: Contact Information
- Attachment: Mail_Check.exe

It installs itself onto the victim machine as

- C:\Mail_Check.exe %Windir%\Mail_Check.exe (where %WinDir% represents the Windows directory)

The following Registry key is set to hook system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ "Mail_Check" = %WinDir%\Mail_Check.exe

The entry below is also added to the Win.ini file as an alternate way for the worm to be run each time a system is restarted:

- run="%Windir%\Mail_Check.exe"

The worm also creates two registry entries as markers to indicate whether it has been run on a machine:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Infected "Name"="Panolili"
"Possessor"="0x06.0x15.0x06.0x09.0x0F.0x0C.0x0F.0x0C"

It will modify the Internet Explorer start page setting in the registry to point to a website for a University in Turkey.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ "Start Page" = http://www.ankara.edu.tr

A VBS script, paket.vbs, is dropped in to the root of the C: drive. This VBS script contains code to initiate a Denial of Service attack against a Turkish Telecom website.

W32/Quaters-A (Win32 Worm): This Internet worm spreads by e-mailing itself to all addresses in the Microsoft Outlook address list and via IRC channels. It attempts to copy itself to C:\PROGRA~1\ACCOUNT_DETAILS.DOC.EXE and adds the following entry to the registry to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ Windows Task Manager = C:\PROGRA~1\ACCOUNT_DETAILS.DOC.EXE

The worm overwrites SCRIPT.INI so that it sends a copy of the worm over IRC channels as a file called CHAIN_MAIL_WORLD_RECORD.IRC. The worm creates the file C:\WIN32.SORT.IT.OUT.BLAIR.TXT and proceeds to overwrite several script files within C:\inetpub\wwwroot with this file. It may attempt a Denial of Service attack on www.number-10.gov.uk. The worm attempts to terminate several processes related to anti-virus and security software, e.g. SWEEP95.EXE, SWNETSUP.EXE, ZONEALARM.EXE, ANTI-TROJANUARYEXE.

W32/Raleka.worm (Aliases: W32/Raleka, Raleka, WORM_RALEKA.A, WORM_RALEKA, Worm.Win32.Raleka, Raleka, W32.HLLW.Raleka, Worm/Raleka.A, Win32/HLLW.Raleka.A, Worm.Win32.Raleka.a, W32/Raleka.A) (Win32 Worm): This is a detection for a new worm exploiting the 'Windows RPC Service' vulnerability (MS03-026 patch). When the worm is executed, it tries to download two files from the IP address 212.59.199.45:

- NTROOTKIT.EXE (128000 bytes)
- NTROOTKIT.REG (245 bytes)

These files are downloaded to the Windows System directory and are detected as "NTRootkit-E." The worm uses its own engine to connect to an IRC Server (IRC.IRCSOULZ.NET:6667) and join a channel. After the worm successfully infects a machine, it tries to overwrite the SVCHOST.EXE in SYSTEM folder and gives the order for the victim machine to download both NTROOTKIT files from the attacking host rather than downloading it from the IP address mentioned above. Finally the IP address of the victim machine is written to a file called "RPCSS.INI" within the Windows System directory on the attacking machine.

W32/Tzet-A (Win32 Worm): When run, this network worm creates the following files in the folder C:\<Windows>\System32: AUTHEXEC.BAT, IGLMTRAY.EXE, IGLXTRAY.EXE, LRSS.INI, NNA.EXE, PRINTF_CORE.EXE, VIDRIV.EXE, WMPT.EXE, WSUBSYS.WAV, XCOPY.DLL. The worm adds the following registry entry to run the file iglmtray.exe when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WUPD

It also searches the local network for computers with weak or no passwords on the administrator or admin accounts to which it can copy itself.

W32/VCK.3037 (Win32 Worm): This encrypted PE file infector virus infects .EXE files in the current directory as well as in the C:\WINDOWS and C:\WINDOWS\SYSTEM directories. Infected files will contain the text "Virus : Win32.FlyPig Author : Vck." This text is encrypted and not directly visible.

W32.Waxpow.Worm (Alias: Bloodhouhd.W32.5) (Win32 Worm): This worm spreads through file sharing networks. It also has Denial of Service (DoS) attack capabilities. It is written in Visual Basic.

W32.Yodo@mm (Alias: W32/Yodo.a@MM) (Win32 Worm): This mass-mailing worm uses its own SMTP engine to spread itself. The e-mail has the following characteristics:

- Subject: Fun game!
- Attachment: flash-game.exe

It is written in the Microsoft Visual Basic programming language.

W32.Zush@mm (Win32 Worm): This mass-mailing worm sends itself to all the addresses in the Microsoft Outlook Address Book.

W97M.Omsec.B (Word 97 Macro Virus): This macro virus spreads by infecting Microsoft Word documents and the global template, Normal.dot. If the day of the month is the 2nd, 11th, or 27th, the virus deletes certain files from the Windows folder.

W97M.Ragaga.A (Word 97 Macro Virus): This simple macro virus spreads to all the open documents and the Microsoft Word global template, Normal.dot.

WORM_AGOBOT.R (Alias: WORM_AGOBOT.R) (Win32 Worm): As a backdoor, this malware connects to an Internet Relay Chat (IRC) server and listens for remote commands. It executes these commands locally on the infected machine, thus providing remote users virtual control over infected systems. This malware propagates only if it is commanded to do so. It may also receive commands that allows it to scan for target systems with the following properties: weak share passwords; vulnerability to the RPC DCOM Buffer Overflow; vulnerability to the Locator Service Buffer Overflow. It copies itself into vulnerable systems and then executes the copy. This malware runs on Windows NT, 2000, and XP.

WORM_RALEKA.B (Aliases: W32/Raleka.B.worm, Worm.Win32.Raleka.B, Raleka.B, W32.HLLW.Raleka, Win32:RPCexploit) (Win32 Worm): This worm employs the RPC_DCOM_Buffer_Overflow vulnerability to spread copies of itself to other machines. It drops and executes a backdoor detected as BKDR_NTRTKIT.A. Additionally, it allows a remote user to gain access to infected machines via Internet Relay Chat (IRC). It runs on Windows 2000 and XP.

XM97/Phone-B (Aliases: Macro.Excel97.Phoneman.b, X97M.Phoneman, X97M_PHONEMAN.A) (Excel 97 macro virus): This variant of XM97/Phone-A that has been modified to contain extra junk routines.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
A97M/AcceV	N/A	Current Issue
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.AntiLam.20.Q	20.Q	Current Issue
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	CyberNotes-2003-16
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	CyberNotes-2003-16
Backdoor.Beasty.Kit	N/A	Current Issue
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.EZBot	N/A	Current Issue
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	CyberNotes-2003-16
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	CyberNotes-2003-16
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04

Trojan	Version	CyberNotes Issue #
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Bobbins	N/A	Current Issue
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Hatter	N/A	Current Issue
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.RPCBot.B:	B	Current Issue
Backdoor.IRC.RPCBot.C	C	Current Issue
Backdoor.IRC.RPCBot.D	D	Current Issue
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lastras	N/A	CyberNotes-2003-17
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Lorac	N/A	CyberNotes-2003-17
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	CyberNotes-2003-16
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Pspider.310.b	310.b	Current Issue
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Rado	N/A	Current Issue
Backdoor.Ranck	N/A	Current Issue
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Roxy	N/A	CyberNotes-2003-16
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Sdbot.P	P	CyberNotes-2003-17
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.Sheldor	N/A	Current Issue
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Sokacaps	N/A	Current Issue
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	CyberNotes-2003-16
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Urat.b	b	Current Issue
Backdoor.Uzbek	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Wolf.16	16	Current Issue
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16

Trojan	Version	CyberNotes Issue #
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciador.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	G	CyberNotes-2003-17
BDS/PowerSpider.A	A	CyberNotes-2003-11
BKDR_LITH.103.A	A	CyberNotes-2003-17
CoolFool	N/A	CyberNotes-2003-17
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Aduent.Trojan	N/A	Current Issue
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Dluca	N/A	CyberNotes-2003-17
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	DN.b	CyberNotes-2003-17
Downloader-EB	EB	Current Issue
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBbot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	N/A	CyberNotes-2003-17
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	N/A	CyberNotes-2003-17
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	N/A	CyberNotes-2003-14
PWS-Aileen	N/A	CyberNotes-2003-04
PWS-Moneykeeper	N/A	Current Issue
PWS-Sincom.dr	dr	CyberNotes-2003-17
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.ALlight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	C	CyberNotes-2003-17
PWSteal.Lemir.D	D	Current Issue
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Train	N/A	CyberNotes-2003-17
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14

Trojan	Version	CyberNotes Issue #
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	1	CyberNotes-2003-14
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Startpage-N	N	CyberNotes-2003-13
Stealthier	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	C	CyberNotes-2003-17
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Bdoor-RQ	RQ	CyberNotes-2003-17
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Golon-A	A	CyberNotes-2003-15
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
Troj/Webber-A	A	CyberNotes-2003-15
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.Analogx	N/A	CyberNotes-2003-17
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Fwin	N/A	Current Issue
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
TrojanGaslid	N/A	Current Issue
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Flipe	N/A	CyberNotes-2003-17

Trojan	Version	CyberNotes Issue #
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovex	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS.Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshe.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32.Igloo-15	N/A	CyberNotes-2003-04
Woodcot	N/A	CyberNotes-2003-16
Xin	N/A	CyberNotes-2003-03

A97M/AcceV (Alias: TR/Macro.Accev): This Trojan attempts to create and execute the file C:\notepad.exe using Windows API functions.

Backdoor.AntiLam.20.Q (Aliases: Backdoor.Antilam.20.q, BackDoor-BQ): This Backdoor Trojan Horse gives its creator access to your computer. By default, it listens on ports 20226 and 52559. The existence of the file nas.exe is in indication of a possible infection. This threat is written in the Delphi programming language.

Backdoor.Beasty.Kit (Aliases: Backdoor.Beastdoor.201, BackDoor-AMQ): This generator program allows a malicious user to create variants of the Backdoor.Beasty Trojan Horse.

Backdoor.EZBot: This Backdoor Trojan Horse allows its creator to use Internet Relay Chat (IRC) to gain access to your computer. The filename of the Trojan may vary. It is written in Microsoft Visual Basic and is packed with PEBundle and UPX.

Backdoor.IRC.Bobbins: This Backdoor Trojan Horse gives its author control of an infected computer through Internet Relay Chat (IRC). The existence of the file windows.exe is an indication of a possible infection. It can update itself by checking for newer versions over the Internet.

Backdoor.IRC.Hatter: This IRC bot connects an infected computer to a specific IRC channel. It may arrive as a self-extracting zip archive that contains six DLLs, an OCX file, and an executable. The executable is written in Microsoft Visual Basic and is packed with ASPack.

Backdoor.IRC.RPCBot.B: This Internet Relay Chat (IRC) Trojan Horse allows its creator to control a computer through IRC. It is also a worm that can use the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) to spread itself.

Backdoor.IRC.RPCBot.C: This Backdoor Trojan Horse gives its creator full control of your computer. The Trojan's creator can also instruct the Trojan to use the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) to spread itself.

Backdoor.IRC.RPCBot.D: This Internet Relay Chat (IRC) Trojan Horse allows its creator to control a computer through IRC. It is also a worm that can use the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) to spread itself.

Backdoor.Pspider.310.b: This variant of Backdoor.PSpider.310 allows unauthorized access to your computer. It contains a keylogger that records all the keystrokes as well as Input/Output (I/O) streams from an infected computer. This threat may be packed with multiple packers, such as ASPack, DBPE, and PECompact.

Backdoor.Rado: This Backdoor Trojan Horse gives its creator unauthorized remote access to your computer. When the Trojan is executed for the first time, it displays a fake error message with the text, "Incompatible Windows Version." It is written in Delphi and may be packed with UPX.

Backdoor.Ranck: This Trojan Horse runs as a proxy server. By default, the Trojan opens port 53201. It is written in Microsoft Visual C++ and is packed with ASPack.

Backdoor.Sheldor (Alias: Backdoor.Sheldor.b): This Backdoor Trojan Horse displays advertisements for an adult Web site. The Trojan Horse is written in the Delphi programming language and is packed with ASPack.

Backdoor.Sokacaps: This Backdoor Trojan Horse is controlled through IRC. While this Trojan allows basic remote control of the victim's machine, it was primarily designed as a tool to perform a Denial of Service (DoS) attack. The Trojan was written in the Microsoft Visual Basic programming language.

Backdoor.Urat.b (Aliases: Backdoor.UltimateRAT.21, BackDoor-PK): This Backdoor Trojan Horse allows unauthorized access to an infected computer. The Trojan listens on port 1012, waiting for a connection from a malicious user. The existence of the file f607.exe is an indication of a possible infection.

Backdoor.Wolf.16 (Aliases: Backdoor.Wolf.16, Backdoor-ABM): This Backdoor Trojan Horse installs itself as a server and allows unauthorized access to an infected computer. It is written in Microsoft Visual C++.

Download.Aduent.Trojan (Aliases: Junksurf.a, VBS_JUNKSURF.A, Downloader-ED, TROJ_JUNKSURF.A): This Trojan Horse downloads and installs the SurferBar Internet Explorer toolbar. The toolbar is downloaded from a hard-coded IP address without your permission. The existence of the file drg.exe is an indication of a possible infection.

Downloader-EB (Alias: TrojanDownloader.Win32.Atmader): This simple downloader Trojan is designed to run on Windows. When run, the Trojan connects to a website (which has been removed), downloads a file to the System directory (typically c:\windows\system32 or c:\windows\system), and executes it. This is the entire purpose of the Trojan.

PWSteal.Lemir.D (Alias: Trojan.PWS.Legendmir.o): This Trojan Horse attempts to steal the password to the "Legend of Mir 2" online game and send it to the creator of the Trojan. It is written in Microsoft Visual C++ and is packed with ASpack v. 2.12.

PWS-Moneykeeper (Alias: Trojan.PSW.Atrar): This Windows-executable Trojan is used by malicious users as a password stealer and a key logger. It attempts to steal Webmoney and system passwords from the infected computer and sends them to the author. Upon execution, the Trojan installs itself into the %Sysdir% directory as Wscrt32.exe. It also drops the keylogger components (MVS RCC.EXE and WFMS CAR.DLL) into the %Sysdir% directory. These files trawl the system and record keystrokes made by the user. There is also an additional file (NSP DOT.EXE) dropped into the %Sysdir% directory. This file checks for certain Webmoney files that may contain user account information. The following Registry key(s) is/are added to hook system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon "Shell" = "Explorer.exe C:\WINNT\System32\wscrt32.exe "
- HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft\Windows NT\CurrentVersion\Winlogon
- "Userinit" = "C:\WINNT\System32\wscrt32.exe "
- The following Registry key(s) is/are added to start the services Start and StaticVxD on NT, Win2K and XP:
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\WCR Values = "Start" and "StaticVxD"
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\MsCRT

Trojan.Fwin: This malicious code modifies the window's registry to make Windows inaccessible. It is written in Visual Basic.

TrojanGaslide: This Trojan Horse attempts to modify the settings in the Internet Explorer Web browser.