



National Infrastructure Protection Center CyberNotes: 2002 Year End Summary

Issue #2002-26

December 30, 2002

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). 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, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a year-end summary of software vulnerabilities identified between December 7, 2001 and December 13, 2002. The table provides the vendor, software name, operating system, common name of the vulnerability, potential risk at the time of publication, and the CyberNotes issue in which the vulnerability appeared. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source indicated in the endnote.** 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	Common Name	Risk*	CyberNotes Issue
0wn f0rum ¹	Multiple	0wn f0rum 2.1	0wn f0rum Script Injection	High	CyberNotes-2002-09
3Com ²	Multiple	Home Connect Cable Modem External with USB	HomeConnect Cable Modem External with USB Denial of Service	Low	CyberNotes 2001-20
3Com ³	Multiple	3CDaemon 2.0 revision 10	3CDaemon Buffer Overflow	High	CyberNotes-2002-09
3Com ⁴	Multiple	Office Connect DSL Router 812 1.1.7, 812 1.1.9	OfficeConnect Port Address Translation Access	Medium	CyberNotes-2002-11
3Com ⁵	Multiple	3Com SuperStack 3 NBX 4.0.17, 4.1.4	3Com SuperStack 3 Denial of Service	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-25
3D3.COM Pty Ltd. ⁶	Windows	Shop Factory 5.5, 5.6	ShopFactory Shopping Cart Cookie Price Manipulation	Medium	CyberNotes-2002-25
4D Inc. ⁷	Windows 98/NT 4.0/2000	WebServer 6.5.7	WebServer Buffer Overflow	High	CyberNotes-2002-10

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
4D Inc. ⁸	Windows 98/NT 4.0/2000, MacOS 8.6/9.0/9.0.4/9.1/9.2/9.2.1/9.2.2	WebServer 6.7.3	WebServer HTTP Request Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-13
Abe Timmerman ⁹	Unix	zml.cgi	zml.cgi File Disclosure	Medium	CyberNotes-2002-01
Abuse ¹⁰	Unix	Abuse 2.0	Abuse Local Buffer Overflows CVE Name: CAN-2002-1250	High	CyberNotes-2002-23
ACD Incorporated ¹¹	Multiple	CwpAPI 1.1	CwpAPI Path Validation	Medium	CyberNotes-2002-02
ACD Systems, Inc. ¹²	Multiple	ACDSee 4.0	ACDSee Photo Album File Description Buffer Overflow	High	CyberNotes-2002-10
acFree Proxy ¹³	Windows NT	acFree Proxy 1.33 -beta7	acFreeProxy Cross-Site Scripting	High	CyberNotes-2002-24
acFTP ¹⁴	Windows NT	acFTP 1.4	acFTP Weak Authentication	Medium	CyberNotes-2002-24
Acme Labs ¹⁵	Unix	thttpd 2.20 b	thttpd Cross-Site Scripting	High	CyberNotes-2002-09
ACME Labs Software ¹⁶	Unix	Tiny HTTPD 0.1.0	TinyHTTPD Directory Traversal	Medium	CyberNotes-2002-23
Activestate ¹⁷	Windows 95/98/ME/NT 4.0/2000, Unix	ActivePerl 5.6.1	ActivePerl Path Revealing	Medium	CyberNotes-2002-01
Activestate ¹⁸	Windows	Active Python 2.1, Activestate win32all	ActivePython Weak Default Security Policy	Medium	CyberNotes-2002-02
Acuma Software Limited ¹⁹	Windows	Acusend 4.0	Acusend Unauthorized File Access	Medium	CyberNotes-2002-22
ACWeb ²⁰	Windows	ACWeb 1.8, 1.14	ACWeb Cross-Site Scripting	High	CyberNotes-2002-20
Ada Core Technologies ²¹	Windows NT 4.0/2000, Unix	Gnat Pro Native 3.12p, 3.13p, 3.14p	Gnat Pro Native Insecure Temporary File	High	CyberNotes-2002-04
Adcycle.com ²²	Unix	Adcycle 1.12-1.17	AdCycle Remote SQL Query Modification	Medium	CyberNotes-2002-01
Add2it ²³	Unix	Mailman Free 1.73	Mailman Free Arbitrary Command Execution	High	CyberNotes-2002-04
Admanager ²⁴	Multiple	Admanager 1.1	Admanager Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-09
Adobe ²⁵	Windows 95/98/ME/NT 4.0/2000, XP	PhotoDeluxe 3.0, 3.1, 4.0	PhotoDeluxe Java Applet	High	CyberNotes-2002-04
Adobe ²⁶	Unix	Acrobat Reader (UNIX) 4.05	Acrobat Reader Insecure Temporary File Creation	Medium	CyberNotes-2002-13
Adobe ²⁷	Windows, MacOS 9	eBook Reader for Mac OS 9 2.1, 2.2, Windows 2.1, 2.2	eBook Reader File Transfer Authorization	Medium	CyberNotes-2002-16
Adobe Systems Inc. ²⁸	Windows	eBook Reader for Windows 2.2	eBook Reader Multiple Vulnerabilities	Low	CyberNotes-2002-15
AeroMail ²⁹	Multiple	AeroMail 0.01.02, 0.01.10, 0.01.20, 0.01.26, 0.01.30, 0.01.40	AeroMail Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-05
Aestiva ³⁰	Multiple	HTML/OS 2.4	HTML/OS Cross-Site Scripting	High	CyberNotes-2002-18
AFD ³¹	Multiple	AFD 1.2-1.2.14	Multiple AFD Working Directory Buffer Overflows	High	CyberNotes-2002-18
AFTPD ³²	Unix	AFTPD 5.4.4	AFTPD Home Directory Change Core Dump	Medium	CyberNotes-2002-01
Agora.cgi ³³	Unix	Agora.cgi 3.3e	Agora.CGI Cross-Site Scripting	High	CyberNotes-2002-01
AHG ³⁴	Multiple	HTML search 1.0	HTML 'Search.CGI' Arbitrary Command	High	CyberNotes-2002-03

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
akfingerd ³⁵	Unix	akfingerd 0.5	Akfingerd Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained)	CyberNotes-2002-25
Aktivate ³⁶	Unix	Aktivate 1.03	Aktivate Shopping Cart Cross-Site Scripting	High	CyberNotes-2002-01.
Aladdin Enterprises ^{37, 38, 39}	Unix	Ghostscript 5.50, 6.51, 6.52	Ghostscript '.locksafes' or '.setsafes' Arbitrary Command Execution CVE Name: CAN-2002-0363	High	CyberNotes-2002-12
Alan Ward ⁴⁰	Windows	A-Cart 2.0	A-Cart Web Accessible Database File	Medium	CyberNotes-2002-18
AlCastle.com ⁴¹	Unix	Aldap 0.09	Aldap Contact Manager Authentication Bypass	High	CyberNotes-2002-25
Alcatel ⁴²	Multiple	Speed Touch Home ADSL	Speed Touch Home ADSL Denial of Service	Low	CyberNotes-2002-02
Alcatel ⁴³	Multiple	OmniPCX 4400	OmniPCX Multiple Vulnerabilities	Low/ Medium (Low if a Denial of Service)	CyberNotes-2002-04
Alcatel ⁴⁴	Multiple	AOS 5.1.1	Alcatel AOS Default Telnet Server Remote Access CVE Name: CAN-2002-1272	High	CyberNotes-2002-24
Alexander Mieland ⁴⁵	Windows, Unix	APBoard 2.0 3, 2.0 2	APBoard Protected Forums & Plaintext Password	Medium	CyberNotes-2002-23
Alguest ⁴⁶	Unix	Alguest 1.0	Alguest Cookie Verification	High	CyberNotes-2002-07
Allaire ⁴⁷	Windows NT 4.0	Forums 2.0.4, 2.0.5, 3.0, 3.1	Forums! Insecure User Validation Message Posting	Medium	CyberNotes-2002-01
Allaire ⁴⁸	Windows 95/98/NT 4.0/2000, Unix	ColdFusion Server 4.0, 4.5, 5.0	ColdFusion DOS Device File Request System Sensitive Information	Medium	CyberNotes-2002-08
Allaire ⁴⁹	Multiple	ColdFusion Server MX Professional, Enterprise Developer	ColdFusion Missing Template Cross Site Scripting	High	CyberNotes-2002-12
Allied Telesyn ⁵⁰	Multiple	AT-8024 1.3.1, Rapier 24	Allied Telesyn Remote Denial of Service	Low	CyberNotes-2002-24
Alsaplayer ⁵¹	Unix	Alsaplayer 0.99.71	Alsaplayer Local Buffer Overflow	High	CyberNotes-2002-20
Alt-N Technologies, LTD ⁵²	Multiple	MDaemon 6.0.0, 6.0.5-6.0.7	MDaemon POP Server Buffer Overflow	Low	CyberNotes-2002-22
Amanda ⁵³	Multiple	Amanda 2.3.0.4	Amanda Multiple Buffer Overflow Vulnerabilities	High	CyberNotes-2002-11
Ambrosia Software ⁵⁴	Unix	Maelstrom GPL 3.0.1	Maelstrom Insecure Symbolic Link	Medium	CyberNotes-2002-02
America OnLine, Inc. ⁵⁵	Windows 95/98/ME/CE/NT 4.0/2000	AOL Instant Messenger 4.0-4.7	AOL Instant Messenger Font Denial of Service	Low	CyberNotes-2002-01
America OnLine, Inc. ⁵⁶	Windows 95/98/ME/NT 4.0/2000, XP	AOL Instant Messenger 4.3-4.8.2616	AOL Instant Messenger Remote Buffer	High	CyberNotes-2002-01
America OnLine, Inc. ⁵⁷	Windows 2000	AOLServer 3.4.2 Win32	AOLServer Password Protected File Arbitrary Read Access	Medium	CyberNotes-2002-01
America OnLine, Inc. ⁵⁸	Multiple	AOL Instant Messenger	AOL Instant Messenger Password Access	Medium	CyberNotes-2002-05
America OnLine, Inc. ⁵⁹	Windows 98/98/ME/NT 4.0/2000, XP, MacOS 9.0	AOL Instant Messenger 2.0N, 2.0.912, 2.0.996, 2.1.1236, 2.5.1598, 2.5.1366, 3.0N, 3.0.1470, 3.0.1415, 3.5.1808, 3.5.1670, 3.5.1635, 3.5.1856, 4.0, 4.1, 4.1.2010, 4.2, 4.2.1193, 4.3, 4.3.2229, 4.4,-4.7, 4.7.2480, 4.8.2616, 4.8.2646	AOL Instant Messenger Denial Of Service	Low	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
America OnLine, Inc. ⁶⁰	Windows 98/ME/NT 4.0/2000, MacOS X 10.x, Unix	AOLServer 3.0, 3.2 Win32, 3.2 Unix, 3.3 Win32, 3.3.1, 3.4 Win32, 3.4, 3.4.2 Win32, 3.4.2	AOLServer Ns_PdLog() Format String	High	CyberNotes-2002-08
America OnLine, Inc. ⁶¹	Windows 95/98/ME/NT 4.0/2000	Instant Messenger 4.0-4.7	AOL Instant Messenger Arbitrary File Creation	Medium	CyberNotes-2002-08
America OnLine, Inc. ⁶²	Windows 95/98/ME/NT 4.0/2000, XP	Instant Messenger 2.0 N, 2.0.912, 2.0.996, 2.1.1236, 2.5 .1598, 2.5.1366, 3.0 N, 3.0 .1470, 3.0.1415, 3.5.1808, 3.5 .1670, 3.5.1635, 3.5.1856, 4.0, 4.1, 4.1.2010, 4.2, 4.2.1193, 4.3, 4.3.2229, 4.5-4.7, 4.7.2480, 4.8.2646, 4.8.2616	Instant Messenger Data Interception	Medium	CyberNotes-2002-09
America OnLine, Inc. ⁶³	Windows 95/98/ME/NT 4.0/2000, XP, Apple MacOS 9.0	Instant Messenger 4.0, 4.1, 4.1.2010, 4.2, 4.2.1193, 4.3, 4.3.2229, 4.4-4.7, 4.7.2480, 4.8.2646, 4.8.2616	Instant Messenger AddBuddy Hyperlink Denial of Service	Low	CyberNotes-2002-10
America OnLine, Inc. ⁶⁴	Windows 95/98/ME/NT 4.0/2000, XP	Instant Messenger 4.2-4.7, 4.7.2480, 4.8.2646, 4.8.2616	Instant Messenger AddExternal App Remote Buffer Overflow	Medium	CyberNotes-2002-10
America OnLine, Inc. ⁶⁵	Windows 95/98/ME/NT 4.0/2000, Mac OS9/X	Instant Messenger 4.5, 4.7, 4.7.2480	AOL Instant Messenger Unauthorized Actions	Medium	CyberNotes-2002-15
America OnLine, Inc. ⁶⁶	Windows 95/98/ME/ NT 4.0/2000, XP	Instant Messenger 4.4-4.7, 4.7.2480, 4.8.2646, 4.8.2616	Instant Messenger Special Character Remote Denial of Service	Low	CyberNotes-2002-17
America OnLine, Inc. ⁶⁷	Windows	Instant Messenger 4.8.2790	AOL Instant Messenger Local File Execution	High	CyberNotes-2002-22
America OnLine, Inc. ⁶⁸	Multiple	Instant Messenger 5.0.2938	AOL Instant Messenger Forced File Download	Medium	CyberNotes-2002-24
America OnLine, Inc. ⁶⁹	Multiple	Instant Messenger 5.1.3036	Instant Messenger Screen Name Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-24
American Power Conversion ⁷⁰	Windows 95/98	Power Chute Plus 5.0.2	PowerChute Plus Insecure Shared Folder Permission	Medium	CyberNotes-2002-13
Analog ⁷¹	Multiple	Analog 3.9 0beta1&2, 4.0 1-4.0 4, 4.1, 4.9 0beta2-4, 4.9 1beta1, 4.11, 4.14-4.16, 5.0-5.0.3, 5.1 a, 5.2	Analog Logfile Script Code Injection	High	CyberNotes-2002-07
AnalogX ⁷²	Multiple	Simple Server: WWW 1.16	SimpleServer: WWW Web Remote Denial of Service	Low	CyberNotes-2002-12
AnalogX ⁷³	Multiple	SimpleServer: Shout 1.0	SimpleServer Shout Buffer Overflow	High	CyberNotes-2002-13
AnalogX ⁷⁴	Multiple	Proxy 4.0, 4.0.1-4.0 7	Proxy Socks4A Buffer Overflow	High	CyberNotes-2002-14
Andrew Bishop ⁷⁵	Multiple	WW -WOFFLE 2.7, 2.7 a, 2.7 b	WWWOFFLE Negative Content-Length Buffer Overflow	High	CyberNotes-2002-15
Andrew G. Morgan ⁷⁶	Unix	Linux PAM 0.76	Linux PAM Authentication Bypass	Medium	CyberNotes-2002-21
AN-HTTPd ⁷⁷	Windows 95/98/ME/ NT 4.0/2000, XP	AN-HTTPd 1.38-140, 1.41, 1.41b, 1.41	AN HTTPD Malformed SOCKS4 Buffer Overflow	High	CyberNotes-2002-22
AN-HTTPd ⁷⁸	Windows 95/98/ME NT 4.0/2000, XP	AN-HTTPd 1.41 d	AN-HTTPD Cross-Site Scripting	High	CyberNotes-2002-22
Annuaire ⁷⁹	Multiple	Annuaire 1.0	Annuaire Sensitive Information	Medium	CyberNotes-2002-09

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Anthill ⁸⁰	Multiple	Anthill 0.1.6.1 & prior	Anthill Multiple Vulnerabilities	Medium/High (High if arbitrary script code can be executed)	CyberNotes-2002-08
Apache Group ⁸¹	Unix	Apache 1.3.11, 1.3.12, 1.3.14, 1.3.17- 1.3.20, 1.3.22	Apache Non-Existent Log Directory Denial Of Service	Low	CyberNotes-2002-01
Apache Group ⁸²	Windows 95/98/NT 4.0/2000	Apache 1.3.11win32-1.3.20win32	Apache Win32 PHP.EXE Remote File Disclosure	High	CyberNotes-2002-01
Apache Group ⁸³	Multiple	Apache 2.0.28 Beta	Apache 'php.exe' Path Disclosure	Medium	CyberNotes-2002-03
Apache Group ⁸⁴	Windows 95/98/NT 4.0/2000, XP	Apache 1.3.6win32, 1.3.9win32, 1.3.11win32-1.3.20 win32; 1.3.22win32, 1.3.23win32, 2.0.28-BETA win32, 2.0.32-BETA win32	Apache Win32 Batch File Command CVE Name: CAN-2002-0061	High	CyberNotes-2002-06
Apache Software Foundation ⁸⁵	Unix	Tomcat 3.0, 3.1, 3.1.1, 3.2, 3.2.1-3.2.4, 3.3, 3.3.1, 4.0, 4.0.1-4.0.3, 4.1	Tomcat Servlet Path Disclosure	Medium	CyberNotes-2002-09
Apache Software Foundation ⁸⁶	Unix	Tomcat 4.1	Tomcat Path Information Disclosure	Medium	CyberNotes-2002-09
Apache Software Foundation ⁸⁷	Unix	Tomcat 3.2.3, 3.2.4	Tomcat Source.JSP Malformed Request	Medium	CyberNotes-2002-11
Apache Software Foundation ⁸⁸	Unix	Tomcat 3.2.3, 3.2.4	Tomcat Example Files Web Root Path Disclosure	Medium	CyberNotes-2002-11
Apache Software Foundation ⁸⁹	Unix	Tomcat 3.2.3, 3.2.4	Tomcat 'RealPath.JSP' Malformed Request	Medium	CyberNotes-2002-11
Apache Software Foundation ⁹⁰	Unix	Tomcat 3.2, 3.2.1, 3.3, 3.3.1, 4.0-4.0.3, 4.1	Tomcat JSP Denial of Service	Low	CyberNotes-2002-12
Apache Software Foundation ⁹¹	Windows 2000	Tomcat 4.0.3	Tomcat Web Root Path Disclosure	Medium	CyberNotes-2002-13
Apache Software Foundation ⁹²	Windows 2000	Tomcat 4.0.3	Apache Tomcat Null Character Malformed Request Denial Of Service	Low	CyberNotes-2002-13
Apache Software Foundation ⁹³	Multiple	Tomcat 4.0.3	Tomcat Multiple Cross-Site Scripting	Low	CyberNotes-2002-14
Apache Software Foundation ⁹⁴	Windows NT 4.0/2000, XP, OS2	Apache 2.0, 2.0.28 -BETA win32, 2.0.28 Beta, 2.0.28, 2.0.32-BETA win32, 2.0.32, 2.0.34 -BETA win32, 2.0.35-2.0.39	Apache Backslash Directory Traversal CVE Names: CAN-2002-0661, CAN-2002-0665	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-17
Apache Software Foundation ⁹⁵	Windows NT 4.0/2000, XP	Apache 2.0, 2.0.28 -BETA win32, 2.0.28 Beta, 2.0.28, 2.0.32 -BETA win32, 2.0.32, 2.0.34 -BETA win32, 2.0.35- 2.0.39	Apache Path Disclosure CVE Name: CAN-2002-0654	Medium	CyberNotes-2002-17
Apache Software Foundation ⁹⁶	Unix	Tomcat 4.1, 4.1.3 beta, 4.1.9 beta	Tomcat Cross-Site Scripting	High	CyberNotes-2002-17
Apache Software Foundation ⁹⁷	Multiple	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.41	Apache 2 mod_dav Remote Denial of Service	Low	CyberNotes-2002-20
Apache Software Foundation ⁹⁸	Unix	Apache 2.0.39, 2.0.40	Apache STDERR Denial of Service	Low	CyberNotes-2002-20
Apache Software Foundation ⁹⁹ <i>Debian releases new advisories</i> ^{100, 101, 102}	Unix	Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17- 1.3.19, 1.3.20, 1.3.22-1.3.27	Multiple Apache Vulnerabilities CVE Name: CAN-2002-1233	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-21 CyberNotes-2002-23
Apache Software Foundation ¹⁰³	Unix	Apache 1.3.26	Apache mod_php File Descriptor Leakage	Medium	CyberNotes-2002-23
Apache Software Foundation ¹⁰⁴	Unix	Apache 1.3, 1.3.11, 1.3.12, 1.3.14, 1.3.17- 1.3.20, 1.3.22- 1.3.27, mod_jk 1.2, Tomcat 4.0-4.0.5, 4.1, 4.1.10, 4.1.12	Apache/ Tomcat Mod_JK Chunked Encoding Denial of Service	Low	CyberNotes-2002-25
Apache Software Foundation ^{105, 106}	Unix	Tomcat 3.0-4.1, 4.1.3 beta, 4.1.9 beta, 4.1.10	Tomcat DefaultServlet File Disclosure	Medium	CyberNotes-2002-20

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
APP ¹⁰⁷	Unix	APBoard 2.0 2	APBoard Unauthorized Thread Reading	Medium	CyberNotes-2002-25
Appalachian State University ¹⁰⁸	Multiple	phpWeb Site 0.8.3	PHPWebSite News Message HTML Injection	High	CyberNotes-2002-20
Appalachian State University ¹⁰⁹	Unix	phpWeb Site 0.8.3	PHPWebSite Article.PHP Cross-Site Scripting	High	CyberNotes-2002-20
Appalachian State University ¹¹⁰	Windows, Unix	PHPWebSite 0.8.2	PHPWebSite Include Statement CVE Name: CAN-2002-1135	High	CyberNotes-2002-20
Apple ¹¹¹	MacOS X 10.0, 10.1, 10.1.1, 10.1.2	MacOS X 10.0-10.1.2	Mac OS X PPP Authentication Credentials Disclosure	Medium	CyberNotes-2002-01
Apple ¹¹²	MacOS X 10.0-10.0.4, 10.1-10.1.2	Palm Desktop 4.0b77, 4.0b76	Palm Desktop For MacOS X Insecure Backup Permissions	Medium	CyberNotes-2002-02
Apple ¹¹³	MacOS 9x	MacOS 9.0, 9.0.4, 9.1, 9.2, 9.2.1, 9.2.2	MacOS 9 DNS Lookup Denial of Service	Low	CyberNotes-2002-04
Apple ¹¹⁴	Windows 95/98/ME/NT 4.0/2000, XP	QuickTime Player for Windows (Japanese) 5.0.1&5.0.2	QuickTime Remote Buffer Overflow	High	CyberNotes-2002-04
Apple ¹¹⁵	Unix	MacOS X 10.1.3	MacOS X 'Sliplogin' Buffer Overflow	Medium	CyberNotes-2002-11
Apple ¹¹⁶	MacOS X 10.x	MacOS X 10.0- 10.0.4, 10.1-10.1.5, MacOS X Server 1.0	MacOS X World Readable Local.NIDump	Medium	CyberNotes-2002-14
Apple ¹¹⁷	MacOS X 10.1x	MacOS X 10.1x	MacOS X Software Update Arbitrary Package Installation CVE Name: CAN-2002-0676	High	CyberNotes-2002-14
Apple ¹¹⁸	MacOS X 10.x	MacOS X 10.0- 10.0.4, 10.1-10.1.5	MacOS iDisk Default Configuration Password Disclosure	Medium	CyberNotes-2002-15
Apple ¹¹⁹	MacOS X 10.2	MacOS X 10.2 (Jaguar)	NetInfo Manager Unauthorized Access	High	CyberNotes-2002-19
Apple ¹²⁰	Windows NT 4.0/2000, XP	QuickTime ActiveX Component 5.0.2	QuickTime ActiveX Component Buffer Overflow CVE Name: CAN-2002-0376	High	CyberNotes-2002-19
Apple ¹²¹	MacOS X 10.2	MacOS X 10.2 (Jaguar)	Mac OS X Terminal.APP Telnet Link	High	CyberNotes-2002-20
Apple ¹²²	MacOs	12/640 Laser Writer TCP/IP Configuration Utility	12/640 PS LaserWriter TCP/IP Telnet Server Password	Medium	CyberNotes-2002-22
Apple ¹²³	MacOS X 10.2	MacOS X 10.2.2, Server 10.2.2	Mac OS X Directory Kernel Panic Denial of Service	Low	CyberNotes-2002-25
Aprelium Technologies ¹²⁴	Windows 95/98/ME/NT 4.0/2000, XP	Abyss Web Server 1.0	Abyss Web Server Administrative Access	High	CyberNotes-2002-08
Aprelium Technologies ¹²⁵	Windows NT	Abyss Web Server 1.0.3	Abyss Web Server HTTP GET Request	Medium	CyberNotes-2002-16
apt-www-proxy ¹²⁶	Unix	apt-www-proxy 0.1	apt-www-proxy NULL HTTP Request Denial of Service & Format String	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-25
Arescom ¹²⁷	Multiple	NET DSL 1000 Series ADSL Router	NetDSL DSL ADSL Router Telnet Denial of Service	High	CyberNotes-2002-04
Arescom ¹²⁸	Multiple	NetDSL 800U	NetDSL DSL Router Administrative Authentication	High	CyberNotes-2002-04
Arescom ¹²⁹	Multiple	NetDSL-800	NetDSL-800 Firmware Undocumented Username/ Password Weakness	Low/ Medium (Medium if configuration settings can be corrupted)	CyberNotes-2002-22
ArGoSoft ¹³⁰	Windows NT 4.0/2000, XP	Mail Server Plus 1.8.1.5, Pro 1.8.1.5	Mail Server Directory Traversal	Medium	CyberNotes-2002-14

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
ArGoSoft ¹³¹	Windows NT 4.0/2000, XP	Mail Server Pro 1.8.1.6, 1.8.1.5, 1.8.1.7	Mail Server Pro Remote Denial of Service	Low	CyberNotes-2002-16
ArGoSoft ¹³²	Windows 95/98/NT 4.0/2000, XP	Mail Server Pro 1.8.1.9	Mail Server Cross-Site Scripting	High	CyberNotes-2002-21
ARSC Really Simple Chat ¹³³	Multiple	ARSC Really Simple Chat 1.0, 1.0.1	ARSC Really Simple Chat Path Disclosure	Medium	CyberNotes-2002-06
Arts Core Studios ¹³⁴	Windows, Unix	CuteCast 1.2	CuteCast Plaintext User Information	Medium	CyberNotes-2002-23
Askey Computer Corporation ¹³⁵	Multiple	ADSL Router RTA-020	ADSL Router Denial of Service	Low	CyberNotes-2002-02
askSam systems ¹³⁶	Multiple	askSam Web Publisher 4.0	askSam Web Publisher Cross-Site Scripting	High	CyberNotes-2002-10
ASPBIn ¹³⁷	Multiple	NewsPro 1.0.1	NewsPro Weak Authentication	High	CyberNotes-2002-10
ASPJar ¹³⁸	Windows NT	Guestbook 1.0	Guestbook Cross-Site Scripting & Path Disclosure	High	CyberNotes-2002-10
ASP-Nuke ¹³⁹	Multiple	ASP-Nuke RC1	ASP-Nuke Image Tag	High	CyberNotes-2002-08
ASP-Nuke ¹⁴⁰	Multiple	ASP-Nuke RC1, RC2	ASP-Nuke Cross-Site Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-08
Astaro ¹⁴¹	Unix	Security Linux 2.016	Security Linux Multiple Vulnerabilities	High	CyberNotes-2002-04
AstroCam ¹⁴²	Unix	AstroCam 1.7.1, 1.8, 1.8.5, 1.8.6, 2.0, 2.1, 2.1.2	AstroCam Shell Metacharacters Sanitization	High	CyberNotes-2002-23
AT&T ¹⁴³	Unix	VNC 3.3.3R2	VNC HTTP Server Denial of Service	Low	CyberNotes-2002-06
atftp ¹⁴⁴	Unix	atftp 0.5, 0.6	ATFTP Buffer Overflow	High	CyberNotes-2002-19
ATGuard ¹⁴⁵	Multiple	Personal Firewall 3.2	Personal Firewall Connection Restriction Bypass	Medium	CyberNotes-2002-09
Atmel ¹⁴⁶	Multiple	Atmel Firmware 1.3	Atmel SNMP public Community or Unknown OID Denial of Service	Low	CyberNotes-2002-01
Atrium Software ¹⁴⁷	Multiple	MERCUR Mailserver 3.3, 3.3 SP1&2, 4.0.1, 4.0.1 SP1, 4.2	MERCUR Mailserver Control-Service Buffer Overflow	High	CyberNotes-2002-15
Authoria ¹⁴⁸	Windows 2000, Unix	HR Suite	HR Suite Cross-Site Scripting	High	CyberNotes-2002-21
Avaya ¹⁴⁹	Multiple	Cajun M770 Supervisor Firmware 3.3, M770-ATM Series Firmware 2.3.11, P130 Series Firmware 2.9.1, P330 Series Firmware 3.8.1, 3.8.2, 3.9.1, 3.10	Cajun Firmware Default Community String	Medium	CyberNotes-2002-16
Avaya ¹⁵⁰	Multiple	IP Office Firmware 1.0	IP Office Malformed Packets Denial of Service	Low	CyberNotes-2002-19
Avaya ¹⁵¹	Multiple	Cajun P550 Series Firmware 4.3.5, P550R Series Firmware 5.2.14, P580 Series Firmware 5.2.14, P880 Series Firmware 5.2.14, P882 Series Firmware 5.2.14	Cajun Firmware Undocumented Default Accounts	Medium	CyberNotes-2002-21
Avaya Labs ¹⁵²	Unix	Libsafe 2.0-9-2.0-11	Libsafe Format String	High	CyberNotes-2002-06
Avenger's News System ¹⁵³	Unix	Avenger's News System 2.01, 2.11	Avenger's News System Directory Traversal and Plugin Subroutine Arbitrary Execution	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-05
Avirt ¹⁵⁴	Windows 95/98/ME/NT 4.0/2000, XP	Gateway 4.2, Suite 4.2, SOHO 4.2	Gateway Suite HTTP and Telnet Remote Buffer Overflow and Telnet Proxy Remote Access	High	CyberNotes-2002-02
Ayman Akt ¹⁵⁵	Unix	IRCIT 0.3.1	IRCIT Remote Buffer Overflow	High	CyberNotes-2002-12
BAL Crew ¹⁵⁶	Windows, Unix	COWS CGI Online Worldweb Shopping 1.1	COWS CGI Online Worldweb Shopping Multiple Vulnerabilities	High	CyberNotes-2002-02

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Balabit ^{157, 158} <i>Engarde releases new patches and SuSE releases patches^{159, 160}</i>	Unix	syslog-ng 1.4 .0rc3, 1.4.7- 1.4.10, 1.4.15, 1.5.15, 1.5.20	Syslog-ng Remote Buffer Overflow CVE Name: CAN-2002-1200	High	CyberNotes-2002-21 CyberNotes-2002-22
Banner Wheel ¹⁶¹	Multiple	Banner Wheel 1.0	BannerWheel Remote Buffer Overflow	High	CyberNotes-2002-11
BasiliX ¹⁶²	Multiple	Webmail 1.10	Webmail Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-13
BB Shareware.Com ¹⁶³	Windows 95/98/NT 4.0/2000	Phusion Webserver 1.0	Phusion Webserver Multiple Vulnerabilities	Low/High (Low for the DoS vulnerability, and High if arbitrary code can be executed)	CyberNotes-2002-04
BBC Education ¹⁶⁴	Multiple	Betsie 1.5-1.5.11	Betsie 'Parser.pl' Cross-Site Scripting	High	CyberNotes-2002-14
BEA Systems ¹⁶⁵	Windows NT 4.0/2000, Unix	WebLogic Server 6.1, 6.1SP1	WebLogic Server DOS Device Denial of Service	Low	CyberNotes-2002-01
BEA Systems ¹⁶⁶	Windows NT 4.0/2000, Unix	WebLogic Server 4.5.2, 4.5.2 SP1&2, 5.1, 5.15.1 SP1-SP9, 6.1, 6.1SP1&2	WebLogic Server URL Parsing Sensitive Information	Medium	CyberNotes-2002-09
BEA Systems ¹⁶⁷	Windows NT 4.0/2000, Unix	WebLogic Server 6.1 SP2	WebLogic Server URL Parsing Path Disclosure	Low/ Medium (Medium if sensitive information is obtained)	CyberNotes-2002-09
BEA Systems ¹⁶⁸	Windows 98/NT 4.0/2000, Unix	WebLogic Express 4.5.1, 4.5.1 SP 15, 4.5.2, 4.5.2SP1&2, 5.1, 5.1 SP1-SP12, 6.0, 6.0SP1&2, 6.1, 6.1SP1&2, Weblogic Server 4.5.1, 4.5.1 SP 15, 4.5.2, 4.5.2SP1&2, 5.1, 5.1SP1-SP12, 6.0, 6.0SP1&2, 6.1, 6.1SP1&2	WebLogic Server and Express File Disclosure	Medium	CyberNotes-2002-10
BEA Systems ¹⁶⁹	Windows 95/98/NT 4.0/2000, Unix	WebLogic Express 5.1, 5.1 SP1-SP12; WebLogic Server 5.1, 5.1 SP1-SP12	WebLogic Server and Express Password Disclosure	Medium	CyberNotes-2002-10
BEA Systems ¹⁷⁰	Windows 95/98/NT 4.0/2000, Unix	WebLogic Express 5.1, 5.1 SP1-6, WebLogic Server 5.1, 5.1 SP1-6	WebLogic Access Controls Bypass	Medium	CyberNotes-2002-13
BEA Systems ¹⁷¹	Windows NT 4.0/2000	WebLogic Server and Express 5.1.x, 6.0.x, 6.1.x and 7.0	WebLogic Server & Express Remote Denial of Service	Low	CyberNotes-2002-14
BEA Systems ¹⁷²	Windows NT 4.0/2000, Unix	WebLogic Express 6.1, 6.1 SP1&2, 7.0.0.1, 7.0, Weblogic Server 6.1, 6.1 SP1&2, 7.0.0.1, 7.0	BEA WebLogic Server and Express HTTP Response Information Disclosure	Medium	CyberNotes-2002-20
BEA Systems ¹⁷³	Windows NT 4.0/2000, Unix	WebLogic Express 7.0.0.1, 7.0; Weblogic Server 7.0.0.1, 7.0	WebLogic Server and Express Inadvertent Security Removal	Medium	CyberNotes-2002-20
BEA Systems ¹⁷⁴	Multiple	WebLogic Express 7.0 SP 1, WebLogic Integration 7.0, 7.0SP1, WebLogic Platform 7.0 SP 1, Weblogic Server 7.0 SP 1	WebLogic Servlet Security Removal	Medium	CyberNotes-2002-21
Belkin ¹⁷⁵	Multiple	F5D5230-4	F5D5230-4 Router Internal Web Request	Medium	CyberNotes-2002-12
Belkin ¹⁷⁶	Multiple	F5D6130	F5D6130 Wireless Network Remote Denial of Service	Low	CyberNotes-2002-18

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Ben Chivers ¹⁷⁷	Unix	Easy Guestbook 1.0	Easy Guestbook Administrative Access	Medium	CyberNotes-2002-16
Ben Chivers ¹⁷⁸	Unix	Easy Homepage Creator 1.0, Advanced Easy Homepage Creator 1.0	Easy Homepage Creator Inadequate Authentication	Medium	CyberNotes-2002-16
Benjamin Lefevre ¹⁷⁹	Unix	Dobermann FORUM 0.1-0.5	Dobermann Forum Remote File Include	Medium	CyberNotes-2002-22
BG Guestbook ¹⁸⁰	Multiple	BG Guestbook 1.0	BG Guestbook Cross-Site Scripting	High	CyberNotes-2002-06
Bharat Mediratta ¹⁸¹	Unix	Gallery 1.1-1.3	Gallery Remote File Include	High	CyberNotes-2002-16
Big Sam ¹⁸²	Multiple	Big Sam 1.1.08	Big Sam Sensitive Information	Medium	CyberNotes-2002-06
BigB ¹⁸³	Multiple	AutoLog 27/07/01	AutoLog IP Spoofing	Medium	CyberNotes-2002-09
BitVise ¹⁸⁴	Windows NT 4.0/2000, XP	WinSSHD 1.1	WinSSHD Denial of Service	Low	CyberNotes-2002-06
BizDesign ¹⁸⁵	Multiple	ImageFolio 2.23, 2.24, 2.26	ImageFolio Unauthorized Administrative Access	High	CyberNotes-2002-12
BizDesign ¹⁸⁶	Multiple	ImageFolio 2.23, 2.24, 2.26, 2.27	ImageFolio Authorized User Web Root Disclosure	Medium	CyberNotes-2002-12
BizDesign ¹⁸⁷	Windows, Unix	ImageFolio 2.23, 2.24, 2.26, 2.27, 3.0.1	ImageFolio Cross-Site Scripting CVE Name: CAN-2002-1334	High	CyberNotes-2002-24
Black Moon ¹⁸⁸	Windows 2000, XP	BlackMoon FTP Server 1.0-1.5	BlackMoon Buffer Overflow	High	CyberNotes-2002-02
Black Tie Project ¹⁸⁹	Multiple	Black Tie Project 0.5b	Black Tie Project Path Disclosure	Medium	CyberNotes-2002-06
Blackboard Inc. ¹⁹⁰	Multiple	Blackboard 5.0	Blackboard Cross-Site Scripting	High	CyberNotes-2002-14
Blahz-DNS ¹⁹¹	Unix	Blahz-DNS 0.2	Blahz-DNS Authentication Bypass	High	CyberNotes-2002-09
Blue Coat Systems ¹⁹²	Multiple	CacheFlow Client Accelerator 4.1.06 & prior, Security Gateway 2.1.02 & prior, Server Accelerator 4.1.06 & prior	Blue Coat Systems Cross-Site Scripting	High	CyberNotes-2002-18
Blue World Communications ¹⁹³	Windows NT	Lasso Web Data Engine 1.6.5	Lasso Web Data Engine Overflow	Low	CyberNotes-2002-04
BlueFace Software ¹⁹⁴	Windows	Falcon Web Server 2.0.0.1020, 2.0.0.1009	Falcon Web Server Authentication Circumvention	Medium	CyberNotes-2002-04
BlueFace Software ¹⁹⁵	Windows	Falcon Web Server 2.0.0.1021 SSL Edition, 2.0.0.1021	Falcon Web Server File Disclosure	Medium	CyberNotes-2002-11.
BlueFace Software ¹⁹⁶	Windows 95/98/NT 4.0/2000, XP	Falcon Web Server 2.0.0.1021 SSL Edition, 2.0.0.1021, 2.0.0.1020, 2.0.0.1009	Falcon Web Server Cross-Site Scripting	High	CyberNotes-2002-17
Boozt! ¹⁹⁷	Unix	Boozt! Standard 0.9.8	Boozt! Buffer Overflow	High	CyberNotes-2002-01
Boozt! ¹⁹⁸	Unix	Boozt! Standard 0.9.8	Boozt index.cgi Buffer Overflow	High	CyberNotes-2002-25
Borland/ Inprise ¹⁹⁹	Unix	Interbase 6.0	Interbase GDS_Lock_MGR & GDS_Drop Buffer Overflow	High	CyberNotes-2002-13
Borland/ Inprise ²⁰⁰	Unix	Interbase 4.0, 5.0, 6.0, 6.5	Interbase GDS_Lock_MGR Buffer Overflow	High	CyberNotes-2002-20
BPM Studio ²⁰¹	Windows 95/98/ME/NT 4.0/2000, XP	BPM Studio Pro 4.2	BPM Studio Pro Directory Traversal	Medium	CyberNotes-2002-05
Bradford Barrett ²⁰²	MacOS X 10.0, Unix	Webalizer 2.0.1 -09, 2.0.1 -06	Webalizer Remote Buffer Overflow	High	CyberNotes-2002-08
Broken bytes ²⁰³	Unix	PhotoDB 1.4	PhotoDB Authentication Script	High	CyberNotes-2002-10
Brother ²⁰⁴	Multiple	NC-3100h	NC-3100H Denial of Service	Low	CyberNotes-2002-16
BrowseFTP ²⁰⁵	Windows 95/NT 4.0	BrowseFTP Client 1.62	BrowseFTP Client Buffer Overflow	High	CyberNotes-2002-01
BRS ²⁰⁶	Windows NT	Web Weaver 1.01	WebWeaver Web Server File Access	Medium	CyberNotes-2002-22
BSCW ²⁰⁷	Windows NT 4.0/2000, Unix	BSCW 3.4, 4.0	BSCW Remote Command Execution and Insecure Default Installation	High	CyberNotes-2002-01
Buffalo Technology ²⁰⁸	Multiple	AirStation Pro Intelligent Access Point WLM-L11G	AirStation Pro Intelligent Access Point Denial of Service	Low	CyberNotes-2002-23

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
bzip2 ²⁰⁹	Unix	bzip2 0.9.5a-d, 0.9.0, 0.9.0a-c, 1.0, 1.0.1	bzip2 Multiple Vulnerabilities	Medium	CyberNotes-2002-11.
bzip2 ²¹⁰	Unix	bzip2 0.9.5a- 0.9.5d, 0.9.0-0.9.0c,1.0, 1.0.1	bzip2 Multiple Vulnerabilities CVE Name: CAN-2002-0759	Medium	CyberNotes-2002-22
CacheFlow ²¹¹	Multiple	CacheOS, 3.1.02- 3.1.20	CacheOS Web Administration Arbitrary Cached Page Code Leakage	Medium	CyberNotes-2002-01
CacheFlow ²¹²	Multiple	CacheOS 3.1.02- 3.1.10, 3.1.20, 3.1, 3.1.11- 3.1.19, 3.1.21, 4.0, 4.0.11- 4.0.14	CacheOS HTTP CONNECT	Medium	CyberNotes-2002-05
CacheFlow ²¹³	Multiple	CacheOS 3.1.17- 3.1.19, 3.1.21, 4.0, 4.0.11- 4.0.14, 4.1.06	CacheOS Cross-Site Scripting	High	CyberNotes-2002-15
Cafelog ²¹⁴	Unix	Cafelog b2 0.6 pre	Cafelog PHP Reference Variable	High	CyberNotes-2002-10
Cafelog ²¹⁵	Multiple	b2 2.6 pre4	b2 WebLog Tool Multiple Vulnerabilities	High	CyberNotes-2002-17
Caldera International, Inc. ²¹⁶	Unix	OpenServer 5.0.5, 5.0.6	OpenServer 'SCOAdmin' Symbolic Link	Medium	CyberNotes-2002-11
Caldera International, Inc. ²¹⁷	Unix	UnixWare 7.1.0	UnixWare CDE DTLogin Log Directory Insecure Permissions	Medium	CyberNotes-2002-01
Caldera International, Inc. ²¹⁸	Unix	UnixWare 7.1.1	UnixWare SCOAdmin Reg.CGI Validation	High	CyberNotes-2002-02
Caldera International, Inc.²¹⁹ <i>Exploit scripts have been published.²²⁰</i>	Unix	UnixWare 7.1.1	UnixWare Library Function	Medium	CyberNotes-2002-03 CyberNotes-2002-04
Caldera International, Inc. ²²¹	Unix	SCO Open Server 5.0.5, 5.0.6	OpenServer dlv_audit Buffer Overflow	High	CyberNotes-2002-06
Caldera International, Inc. ²²²	Unix	nscd 2.2.4	nscd Incorrect Hosts Cache Behavior	Medium	CyberNotes-2002-07
Caldera International, Inc. ²²³	Unix	OpenLinux Server 3.1.1, OpenLinux Workstation 3.1.1	OpenLinux StartKDE Script LD LIBRARY PATH	Medium	CyberNotes-2002-07
Caldera International, Inc. ²²⁴	Unix	XFree86 X11R6 4.0.2 -11, 4.1 -11	XFree86 MIT-SHM	Medium	CyberNotes-2002-07
Caldera International, Inc. ²²⁵	Unix	OpenUnix 8.0; UnixWare 7.1.1	Caldera X11 Library -xrm Buffer Overflow	High	CyberNotes-2002-08
Caldera International, Inc. ²²⁶	Unix	OpenServer 5.0.5, 5.0.6	OpenServer popper Denial of Service	Low	CyberNotes-2002-11
Caldera International, Inc. ²²⁷	Unix	OpenServer 5.0.5, 5.0.6	OpenServer crontab Format String	High	CyberNotes-2002-12
Caldera International, Inc. ²²⁸	Unix	OpenUnix 8.0, UnixWare 7.1.1	Open Unix / UnixWare ftpd PASV Mode Hijacking	Medium	CyberNotes-2002-12
Caldera International, Inc. ²²⁹	Unix	Volition Manager 1.1	Volition Manager Unencrypted Password	Medium	CyberNotes-2002-12
Caldera International, Inc. ²³⁰	Unix	OpenUnix 8.0, UnixWare 7.1.1	UnixWare / Open UNIX pptalk Privilege Escalation	High	CyberNotes-2002-13
Caldera International, Inc. ²³¹	Unix	OpenUnix 8.0, UnixWare 7.1.1	Caldera X 'xkbcomp' Vulnerabilities	High	CyberNotes-2002-18
Caldera International, Inc. ²³²	Unix	UnixWare 7.1.0, 7.1.1	UnixWare Information Disclosure	Medium	CyberNotes-2002-04
Caldera International, Inc. ²³³	Unix	OpenUnix 8.0; UnixWare 7.1.1	OpenUnix DTTmpDir World Writeable Directories Permissions	Medium	CyberNotes-2002-10
Caldera International, Inc. ²³⁴	Unix	OpenUnix 8.0; UnixWare 7.1.1	UnixWare/ OpenUnix Proc File System Denial of Service CVE Name: CAN-2002-1231	Low	CyberNotes-2002-22
Calisto ²³⁵	Unix	Internet Talker 0.4	Internet Talker Remote Denial of Service	Low	CyberNotes-2002-24

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Canna ²³⁶	Unix	Canna 3.5 b2	Canna Server Local Buffer Overflow CVE Names: CAN-2002-1158, CAN-2002-1159	High	CyberNotes-2002-25
CARE 2002 ²³⁷	Unix	CARE 2002 1.0.01 & prior	CARE 2002 Multiple Vulnerabilities	Medium	CyberNotes-2002-15
Carlos Sanchez Valle ²³⁸	Multiple	MyNews Groups :) 0.4, 0.4.1	MyNews Groups Subject Header	Medium	CyberNotes-2002-20
Carnegie Mellon University ²³⁹	Unix	Cyrus IMAP Server 1.4, 2.1.10	Cyrus IMAPD Pre-Login Buffer Overflow	High	CyberNotes-2002-25
Cascade Soft ²⁴⁰	Unix	W3Mail 1.0.2-1.0.5	W3Mail Predictable File Attachment Location	Medium	CyberNotes-2002-15
Cascade Soft ²⁴¹	Multiple	W3Mail 1.0.6 & greater	W3Mail File Disclosure	Medium	CyberNotes-2002-23
Castelle ²⁴²	Multiple	FaxPress Software 6.3	FaxPress Password Disclosure	Medium	CyberNotes-2002-03
Caucho Technology ²⁴³	Windows 2000	Resin 2.0, 2.1.1, 2.1.2	Resin Server 'view_source' Directory Traversal	Medium	CyberNotes-2002-13
Caucho Technology ²⁴⁴	Windows 2000	Resin 2.1.1	Resin Server Denial of Service	Low	CyberNotes-2002-13
Caucho Technology ²⁴⁵	Windows 2000	Resin 2.1.1	Resin Server DOS Device Denial of Service	Low	CyberNotes-2002-13
Caucho Technology ²⁴⁶	Windows 2000	Resin 2.1.1, 2.1.2	Resin Server Device Name Path Disclosure	Medium	CyberNotes-2002-15
Caupo.net ²⁴⁷	Multiple	CaupoShop 1.30rc4, 1.30a	CaupoShop Cross-Site Scripting	High	CyberNotes-2002-06
CDRDAO ²⁴⁸	Unix	CDRDAO 1.1.4, 1.1.5	CDRDAO Configuration File Symbolic Link	High	CyberNotes-2002-02
Century Software ²⁴⁹	Unix	Term For Linux 0.06.27.0869	Term Buffer Overflow	High	CyberNotes-2002-05
Cerulean Studios ²⁵⁰	Windows 95/98/ME/NT 4.0/2000	Trillian 0.73, 0.725, 0.6351	Trillian Buffer Overflows	High	CyberNotes-2002-16
Cerulean Studios ²⁵¹	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.725, 0.6351	Trillian Skins Colors Buffer Overflow	Low/High (High if arbitrary code is executed)	CyberNotes-2002-18
Cerulean Studios ²⁵²	Windows 95/98/ME NT 4.0/2000	Trillian 0.73, 0.725, 0.6351	Trillian Weak Password Encryption	Medium	CyberNotes-2002-19
Cerulean Studios ²⁵³	Windows	Trillian 0.73, 0.74	Trillian IRC PRIVMSG Buffer Overflow	Low/High (High if arbitrary code is executed)	CyberNotes-2002-19
Cerulean Studios ²⁵⁴	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.74, 0.725, 0.6351	Trillian Identd Buffer Overflow	Low/High (High if arbitrary code is executed)	CyberNotes-2002-19
Cerulean Studios ²⁵⁵	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.74	Trillian JOIN Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Cerulean Studios ²⁵⁶	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.74	Trillian AIM Remote Denial of Service	Low	CyberNotes-2002-20
Cerulean Studios ²⁵⁷	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.74, 0.725	Trillian IRC Raw 221 Requests Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Cerulean Studios ²⁵⁸	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.74	Trillian Multiple IRC Denial of Service Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
CGIScript.net ²⁵⁹	Unix	csBanner 1.0, csCreate Pro 1.0, csDown-load 1.0, csFAQ 1.0, csFiler 1.0, csFileshare 1.0, csGrid 1.0, csIncludes 1.0, csMailto, csNews 1.0, csNews Professional 1.0, csRandom Text 1.0, csUpload 1.0	CGIScript.net Information Disclosure	Medium	CyberNotes-2002-11
CGIScript.net ²⁶⁰	Unix	CSSearch 2.5 & prior	CSSearch Remote Command Execution	High	CyberNotes-2002-07
CGIScript.net ²⁶¹	Unix	CSGuest book 1.0, CSLive Support 1.0, CSNews Professional 1.0, CSChat-R-Box 1.0	CS Guestbook Remote Command Execution	High	CyberNotes-2002-08
CGIScript.net ²⁶²	Multiple	csMailto	csMailto Remote Command Execution	High	CyberNotes-2002-09
CGIScript.net ²⁶³	Multiple	csNews 1.0, csNews Professional 1.0	csNews Multiple Vulnerabilities	Medium	CyberNotes-2002-12
CGIScript.net ²⁶⁴	Unix	csPassword 1.0	csPassword Multiple Vulnerabilities	Medium	CyberNotes-2002-12
Check Point Software Technologies ²⁶⁵	Multiple	Firewall-1 4.0, 4.0SP1-8, 4.1, 4.1SP1-5; Next Generation 0.0; VPN-1 4.1, 4.1SP1-4	FW-1 SecuClient/ SecuRemote Security Bypass	Medium	CyberNotes-2002-06
Check Point Software Technologies ²⁶⁶	Multiple	VPN-1 4.1, 4.1 SP1-SP4	VPN-1 IKE Security Restriction Bypass	Medium	CyberNotes-2002-21
Check Point Software Technologies ²⁶⁷	Multiple	Firewall-1 4.0, 4.0 SP1-SP8, 4.1, 4.1 SP1-SP5, Firewall-1 (VPN+ DES + STRONG)] 4.1 SP2 Build 41716, 4.1 Build 41439, (VPN + DES) 4.1, Next Generation, Next Generation FP1&FP2	Check Point Firewall-1 SecuRemote IKE Username Guessing	Medium	CyberNotes-2002-18
Check Point Software Technologies ²⁶⁸	Multiple	Firewall-1 4.1, 4.1 SP1-SP6, Next Generation, Next Generation FP1&FP2	Firewall-1 HTTP Proxy Server	Medium	CyberNotes-2002-19
Cherokee ²⁶⁹	Unix	Cherokee HTTPD 0.2.0-0.2.6, 0.15- 0.1.6, 0.1.0	Cherokee HTTPD Multiple Vulnerabilities	Medium/High (High for the root privileges and unfiltered meta-character vulnerabilities.)	CyberNotes-2002-01
Chinput ²⁷⁰	Unix	Chinput 3.0	Chinput Environment Variable Buffer Overflow	High	CyberNotes-2002-02
Christof Pohl ^{271, 272}	Unix	Improved mod_front page 1.3.1, 1.3.2, 1.4.1, 1.5, 1.5.1	Improved mod_frontpage Buffer Overflow	High	CyberNotes-2002-06
chuid ²⁷³	Multiple	chuid 1.0-1.2	CHUID File Input Validation	Medium	CyberNotes-2002-02
CIDER ²⁷⁴	Unix	Shadow 1.5, 1.6	Shadow Remote Command Execution CVE Name: CAN-2002-0091	High	CyberNotes-2002-09
Cisco Systems ²⁷⁵	Windows 95/98/ME/NT 4.0/2000	Cisco SN 5420 Storage Router 1.1(2)-(5)	Cisco SN 5420 Storage Router Multiple Vulnerabilities	Low/ Medium	CyberNotes-2002-01
Cisco Systems ²⁷⁶	Multiple	Cisco ubr920, ubr924, ubr925	Cisco Cable Access Router MIB Community Default Passwords	Medium	CyberNotes-2002-01
Cisco Systems ²⁷⁷	Unix	Billing and Management Server, PGW 2200, SC2200, Voice Services Provisioning Tool, VSC3000	Cisco Media Gateway Controller Vulnerability Exposure	High	CyberNotes-2002-02
Cisco Systems ²⁷⁸	Unix	tac_plus F4.0.4 alpha	Tac_Plus Insecure Accounting File	Medium	CyberNotes-2002-03

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Cisco Systems ²⁷⁹	Multiple	Detailed list available at: http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml	IOS Malformed SNMP Message Denial of Service	Low	CyberNotes-2002-04
Cisco Systems ²⁸⁰	Multiple	IOS 11.1CC, 12.0T, 12.0ST, 12.0S, 12.0, 12.1T, 12.1E, 12.1, 12.2T, +12.2	Cisco IOS CEF Sensitive Information	Medium	CyberNotes-2002-05
Cisco Systems ²⁸¹	Multiple	Call Manager 3.0, 3.1	CallManager CTI Denial of Service	Low	CyberNotes-2002-07
Cisco Systems ²⁸²	Windows NT 4.0/2000	Cisco Secure ACS for Windows NT 2.6, 2.6.2, 2.6.3, 2.6.4, 3.0.1, 3.0	CiscoSecure ACS Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-07
Cisco Systems ²⁸³	Multiple	AP340, AP350, BR350	Cisco Aironet Telnet Authentication Denial of Service	Low	CyberNotes-2002-08
Cisco Systems ²⁸⁴	Windows XP	VPN Client 3.1 & 3.5.1 for Windows	VPN Client for Windows Dialog Instructions	Medium	CyberNotes-2002-09
Cisco Systems ²⁸⁵	Multiple	ATA-186	ATA-186 HTTP Device Configuration Disclosure & Web Administration Authentication Bypass	Medium	CyberNotes-2002-10
Cisco Systems ²⁸⁶	Multiple	Cache Engine 505, 505 2.2.0, 505 3.0&4.0, 550, 550 2.2.0, 550 3.0&4.0, 570, 570 2.2.0, 570 3.0&4.0; Content Distribution Manager 4630, 4630 4.0&4.1, 4650, 4650 4.0&4.1; Content Engine 507, 507 2.2.0, 507 3.1, 507 4.0&4.1, 560, 560 2.2.0, 560 3.1, 560 4.0&4.1, 590, 590 2.2.0, 590 3.1, 590 4.0&4.1, 7320, 7320 2.2.0, 7320 3.1, 7320 4.0&4.1, 4430, 4430 4.0&4.1	Cache Engine Default Access Control	Medium	CyberNotes-2002-10
Cisco Systems ²⁸⁷	Multiple	IDS Device Manager 3.1.1	IDS Device Manager Directory Traversal	Medium	CyberNotes-2002-10
Cisco Systems ²⁸⁸	Multiple	IOS software (all versions), Media Gateway Controller (MGC) and related products, BTS 10200, Cisco IP Manager	IOS Software NTP Buffer Overflow	High	CyberNotes-2002-10
Cisco Systems ²⁸⁹	Multiple	WebNS 4.0 1.053s, 5.02.005s, 5.0 1.012s, 5.0 0.038s, 5.1 0.0.10	WebNS Denial of Service Vulnerabilities	Low	CyberNotes-2002-10
Cisco Systems ²⁹⁰	Multiple	Catalyst 4000 5.5.5, 6.3.5, 7.1.2	Catalyst Unicast Traffic Broadcast	Medium	CyberNotes-2002-11
Cisco Systems ²⁹¹	Multiple	CBOS 2.3.9, 2.3.8, 2.3.7.002, 2.3.7, 2.3.5.015, 2.3.5, 2.3.2, 2.2.1a, 2.2.1, 2.2.0, 2.1.0a, 2.1.0, 2.0.1, 2.3 .053, 2.3, 2.4.1, 2.4.2b, 2.4.2ap, 2.4.2, 2.4.3, 2.4.4	Cisco Broadband Operating System Remote Denial of Service Vulnerabilities	Low	CyberNotes-2002-11
Cisco Systems ²⁹²	Multiple	IOS 11.0 (22a), (18), IOS 11.1 (24a), IOS 11.3 (11b), IOS 12.0 (3)	IOS ICMP Redirect Denial Of Service	Low	CyberNotes-2002-11
Cisco Systems ²⁹³	Multiple	VoIP Phone CP-7910 3.0-3.2, CP-7940 3.0-3.2, CP-7960 3.0-3.2	VoIP Phone Stream Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information and unauthorized access can be obtained)	CyberNotes-2002-11
Cisco Systems ²⁹⁴	Multiple	All devices running Cisco IOS® Software supporting SSH; Catalyst 6000 switches running CatOS; PIX Firewall; Cisco 11000 Content Service Switch family	Cisco SSH Denial of Service	Low	CyberNotes-2002-13

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Cisco Systems ²⁹⁵	Multiple	IOS 11.3 XA, 11.3 T, 11.3 NA, 12.0 XR, 12.0 T, 12.0 SC, 12.0, 12.1T, 12.1 EC, 12.1 CX, 12.1, 12.2 XF, 12.2 T, 12.2 BC, 12.2	Cisco Cable Modem Termination System Authentication Bypass	Medium	CyberNotes-2002-13
Cisco Systems ²⁹⁶	Multiple	ONS 15454 Optical Transport Platform 3.1.0, 3.2.0	ONS 15454 Remote Denial of Service	Low	CyberNotes-2002-13
Cisco Systems ²⁹⁷	Windows NT 4.0/2000	Secure ACS for Windows NT 3.0, 3.0.1	Cisco Secure ACS Cross-site Scripting	High	CyberNotes-2002-13
Cisco Systems ²⁹⁸	MacOS X, Unix	VPN Client 3.5.1 for Solaris, 3.5.1 for Mac OS X, 3.5.1 for Linux	VPN Client Buffer Overflow	High	CyberNotes-2002-13
Cisco Systems ²⁹⁹	Multiple	IntraPort 2, 2+, Carrier-2, Carrier-8, Enterprise-2, 8, VPN 5001 Concentrator, VPN 5002 Concentrator, VPN 5008 Concentrator	VPN 5000 Concentrator Plaintext	Medium	CyberNotes-2002-16
Cisco Systems ³⁰⁰	Multiple	IOS 11.1-11.3	IOS TFTP Buffer Overflow	Low	CyberNotes-2002-16
Cisco Systems ³⁰¹	Windows, MacOS X 10.1.x, Unix	VPN Client 3.5.1 for Windows, Solaris, Mac OS X, Linux, 3.5.2 for Solaris, Mac OS X, Linux	VPN Client Multiple IKE Packet Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-17
Cisco Systems ³⁰²	Multiple	Cisco VPN 3000 Concentrator 2.5.2 (A)-(C) & (F), 3.0.3 (A), 3.1.1, 3.5 (Rel), 3.5.3, 3.5.4, 3.6 (Rel), VPN 3002 Hardware Client	Multiple Cisco VPN 3000 Vulnerabilities	Low/ Medium (Medium if unauthorized access is obtained or sensitive information is obtained)	CyberNotes-2002-18
Cisco Systems ³⁰³	Windows	VPN Client 2.0, 3.0 for Windows	Cisco VPN Client NETBIOS TCP Remote Denial of Service	Low	CyberNotes-2002-18
Cisco Systems ³⁰⁴	Windows, Unix, MacOS X 10.1.0 or later	VPN Client 2.0, 3.0, 3.0.5, 3.1, 3.5.1 for Windows, VPN Client 3.5.1 for Solaris, 3.5.1 for Mac OS X, 3.5.1 for Linux	VPN Client Distinguished Name Validation	Medium	CyberNotes-2002-18
Cisco Systems ³⁰⁵	Windows, Unix, MacOS X 10.1.0 or later	VPN Client 2.0, 3.0, 3.0.5, 3.1, 3.5.1C, 3.5.1 for Windows, VPN Client 3.5.1, 3.5.2 for Solaris, VPN Client 3.5.1, 3.5.1 for Mac OS X, VPN Client 3.5.1, 3.5.2 for Linux	VPN Client Random Number Generation	Medium	CyberNotes-2002-18
Cisco Systems ³⁰⁶	Windows, Unix, MacOS X 10.1.0 or later.	VPN Client 2.0, 3.0, 3.0.5, 3.1, 3.5.1C, 3.5.1,3.5.2, 3.6 (Rel), 3.6 for Windows, VPN Client 3.5.1, 3.5.2, 3.6 for Solaris, 3.5.1, 3.5.2, 3.6 for Mac OS X, VPN Client 3.5.1, 3.5.2, 3.6 for Linux	VPN Client All Tunnel Mode Information Leakage	Medium	CyberNotes-2002-18
Cisco Systems ³⁰⁷	Windows	VPN Client 2.0, 3.0, 3.1, 3.5.1 for Windows	VPN Client Password Disclosure	Medium	CyberNotes-2002-18
Cisco Systems ³⁰⁸	Multiple	IP Phone 7960	IP Phone 7960 Unsigned Content Weakness	Medium	CyberNotes-2002-19
Cisco Systems ³⁰⁹	Unix	VPN 5000 Client for Linux 5.2.6, VPN 5000 Client for Solaris 5.2.7	VPN 5000 Client Buffer Overflow Vulnerabilities	High	CyberNotes-2002-19
Cisco Systems ³¹⁰	Mac OS	VPN 5000 Client for Mac OS 5.1.2, Mac OS 5.2.1	Mac OS VPN 5000 Client Password Disclosure	Medium	CyberNotes-2002-19
Cisco Systems ³¹¹	Multiple	CatOS 5.4, 5.5 (13a), 5.5, 6.1 (2), 6.1, 7.3, 7.4	CatOS CiscoView Remote Denial of Service	Low	CyberNotes-2002-21
Cisco Systems ³¹²	Multiple	Unity Server 2.0-2.4, 2.46, 3.0, 3.1	Cisco Unity Predefined Restriction Tables CVE Names: CAN-2002-1189, CAN-2002-1190	Medium	CyberNotes-2002-21

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Cisco Systems ³¹³	Multiple	ONS 15327 3.0-3.3, ONS 15454 Optical Transport Platform 3.0, 3.1.0, 3.2.0, 3.3	Cisco ONS15454/ONS15327 Optical Transport Platforms Multiple Vulnerabilities	Medium/ High (High if complete control can be obtained)	CyberNotes-2002-22
Cisco Systems ³¹⁴	Multiple	PIX Firewall 6.2.2	PIX Firewall Denial of Service	Low/High (High if DDoS best practices not in place)	CyberNotes-2002-23
Cisco Systems ³¹⁵	Multiple	PIX Firewall 5.0, 5.1, 5.1 (4.206), 5.1.4, 5.2, 5.2 (2), 5.2 (3.210), 5.2 (5), (6), (7), 6.0, 6.0 (1), (2), 6.0.3, 6.1, 6.1 (2), 6.1.3, 6.2, 6.2 (1), 6.2.1	PIX TACACS+/ RADIUS HTTP Proxy Buffer Overrun	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-24
Cisco Systems ³¹⁶	Multiple	PIX Firewall 6.0, 6.0 (1), 6.0 (2), 6.0.3, 6.1, 6.1 (2), 6.1.3	PIX Firewall VPN Session	Medium	CyberNotes-2002-24
Cisco Systems ³¹⁷	Multiple	Cisco 7600, Catalyst 6500 , IOS 12.1 (9)E, (8)E, (13.4)E, (12)E, (11)E, (10)E	Cisco OSM Line Card Header Corruption	Low	CyberNotes-2002-25
Cisco Systems ³¹⁸	Windows NT 4.0/2000	Secure ACS for Windows NT 3.0.1	Secure ACS NDS Expired/ Disabled User Authentication	Medium	CyberNotes-2002-03
Citadel/UX ³¹⁹	Unix	Citadel/UX 5.90	Citadel/UX Denial of Service	Low	CyberNotes-2002-06
Citrix Systems, Inc. ³²⁰	Windows, MacOS, Unix	ICA Client for Windows 6.1	Citrix ICA Client Automatic Remote Code Execution	High	CyberNotes-2002-01
Citrix Systems, Inc. ³²¹	Multiple	Nfuse 1.6	Nfuse 'applist.asp' Information Leak	Medium	CyberNotes-2002-02
Citrix Systems, Inc. ³²²	Multiple	Nfuse 1.6	NFuse Network Sensitive Information	Medium	CyberNotes-2002-04
Citrix Systems, Inc. ³²³	Multiple	Nfuse 1.5	Nfuse boilerplate.asp Directory Traversal	Medium	CyberNotes-2002-07
Citrix Systems, Inc. ³²⁴	Multiple	Nfuse 1.51, 1.6	NFuse Cross-Site Scripting	High	CyberNotes-2002-07
Citrix Systems, Inc. ³²⁵	Windows NT 4.0	MetaFrame for Windows NT 4.0 TSE 1.8	Metaframe Remote Denial of Service	Low	CyberNotes-2002-17
Citrix Systems, Inc. ³²⁶	Windows 2000	MetaFrame XP, XP SP1&2	Citrix MetaFrame Client-Specified Published Applications	High	CyberNotes-2002-20
Citrix Systems, Inc. ³²⁷	Windows 2000	MetaFrame XPs, XPe, XPa, XP, MetaFrame	Citrix Information Disclosure	Medium	CyberNotes-2002-21
ClanLib ³²⁸	Unix	ClanLib 5.0	ClanLib Environment Variable	High	CyberNotes-2002-02
Claymore Systems, Inc. ³²⁹	Multiple	PureTLS 0.9b1	PureTLS Injection Attack	Medium	CyberNotes-2002-06
Click2 Learn ³³⁰	Multiple	Ingenium Learning Management System 5.1, 6.1	Ingenium Learning Management System Multiple Vulnerabilities	Medium	CyberNotes-2002-21
Clicky Web ³³¹	Multiple	Pseudo-frames 1.0	Pseudo-frames Remote File Include	High	CyberNotes-2002-10
C-Note ³³²	Unix	mysql_auth_ldap 1.0.1, 1.0.2 -beta, 1.2 b1, 1.2, 2.0 b4, 2.0 b3, 2.0 b1, 2.0, 2.0.1	Squid_Auth_LDAP Pam Logging Format String	Low	CyberNotes-2002-10
Cobalt ³³³	Unix	Qube 3.0	Cobalt Qube Authentication Bypass	High	CyberNotes-2002-15
ComCity Corporation ³³⁴	Windows 95/98/ME/NT 4.0/2000, XP	SalesCart Pro 1.0, 1.5, 3.0, SalesCart-STD 1.2, 2.0	SalesCart Customer Database Disclosure	Medium	CyberNotes-2002-13
Common Name ³³⁵	Windows	Common Name Toolbar 3.5.2 .0	CommonName Toolbar Potential Information Leakage	Medium	CyberNotes-2002-20
Compaq Computer Corporation ³³⁶	Multiple	Nonstop Kernel S-Series 3.0	Nonstop Himalaya SNMP Agent Denial Of Service	Low	CyberNotes-2002-04

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Compaq Computer Corporation ³³⁷	Multiple	TCP/IP Services For OpenVMS 5.3, Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1	Compaq SNMP Denial of Service	Low/ Medium (Medium if unauthorized access is obtained)	CyberNotes-2002-04
Compaq Computer Corporation ³³⁸	Multiple	ACMS 4.3, 4.4	ACMS Unauthorized Access	Medium	CyberNotes-2002-05
Compaq Computer Corporation ³³⁹	Unix	Tru64 4.0 g PK3 (BL17), Tru64 4.0 f PK7 (BL18), Tru64 5.0 a PK3 (BL17), Tru64 5.0, Tru64 5.1 a PK1 (BL1), Tru64 5.1 PK4 (BL18), Tru64 5.1	Compaq Tru64 C Library Buffer Overflow	Medium	CyberNotes-2002-08
Compaq Computer Corporation ³⁴⁰	Multiple	Integrated Administrator firmware 1.0, 1.10	Integrated Administrator Firmware Unauthorized Access	High	CyberNotes-2002-11
Compaq Computer Corporation ³⁴¹	Unix	Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1	Tru64 IPCS Buffer Overflow CVE Name: CAN-2002-0093	High	CyberNotes-2002-15
Compaq Computer Corporation ³⁴²	Unix	Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1	Tru64 InetD Denial of Service	Low	CyberNotes-2002-15
Compaq Computer Corporation ³⁴³ <i>Patches now available³⁴⁴</i>	Unix	Tru64 5.0, 5.0 a, 5.1, 5.1 a	Tru64 SU Buffer Overflow	High	CyberNotes-2002-15 CyberNotes-2002-16
Compaq Computer Corporation ³⁴⁵	Unix	Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1	Tru64 Multiple Vulnerabilities	High	CyberNotes-2002-16
Compaq Computer Corporation ³⁴⁶	Unix	Digital Unix 4.0f, Tru64 4.0g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f PK6 (BL17), 4.0f, 5.0a PK3 (BL17), 5.0a, 5.0 PK4 (BL17 & 18), 5.1a PK2 (BL2), 5.1a PK1 (BL1), 5.1a, 5.1 PK5 (BL19), 5.1 PK4 (BL18), 5.1 PK3 (BL17), 5.1	Tru64 UNIX Multiple Local and Remote Buffer Overflow	Low/High (High if arbitrary code is executed)	CyberNotes-2002-18
Compaq Computer Corporation ³⁴⁷	Unix	Tru64 4.0g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f PK6 (BL17), 4.0f, 5.0a PK3 (BL17), 5.0a	HP Tru64 Initial Random TCP Sequence Number Denial of Service	Low	CyberNotes-2002-19
Compaq Computer Corporation ³⁴⁸	Unix	Tru64 4.0g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f PK6 (BL17), 4.0f, 5.0f, 5.0a PK3 (BL17), 5.0a, 5.0 PK4 (BL18), 5.0 PK4 (BL17), 5.0, 5.1a PK1 (BL1), 5.1a, 5.1 PK4 (BL18), 5.1 PK3 (BL17), 5.1	Tru64 Address Resolution Protocol	Low/ Medium (Low if a Denial of Service)	CyberNotes-2002-19
Compaq Computer Corporation ³⁴⁹	Multiple	Compaq TCP/IP Services For OpenVMS 4.2, 5.0 a, 5.1, 5.3	OpenVMS UCX POP Server	Medium	CyberNotes-2002-20
Compaq Computer Corporation ³⁵⁰	Windows NT 4.0/2000, XP, Unix	HP WEBES Service Tools 2.0, 3.1, 4.0, 4.0 SP1-SP50	HP WEBES Service Tools Unauthorized File Access	Medium	CyberNotes-2002-20
Compaq Computer Corporation ³⁵¹	Multiple	Insight Management Agents 4.2, 4.37	HP Compaq Insight Manager Web Interface Cross-Site Scripting	High	CyberNotes-2002-20
Compaq Computer Corporation ³⁵²	Unix	Tru64 4.0 g PK3 (BL17), 4.0f PK7 (BL18), 5.0a PK3 (BL17), 5.1a PK3 (BL3), 5.1 PK5 (BL19)	Tru64 IGMP Denial of Service	Low	CyberNotes-2002-23
Compaq Computer Corporation ³⁵³	Windows 98/ME/ 2000	Intel PRO/ Wireless 2011B LAN USB Device Driver 1.5.16.0, 1.5.18.0	Intel PRO/Wireless 2011B LAN USB Device Driver Plaintext WEP	Medium	CyberNotes-2002-03
Compaq Computer Corporation ³⁵⁴	Unix	Tru64 4.0d	Tru64 Scan Denial Of Service	Low	CyberNotes-2002-03
Compaq Computer Corporation ³⁵⁵	Unix	Tru64 4.0g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f PK6 (BL17), 4.0f, 4.0d PK9 (BL17), 4.0d, 5.0a PK3 (BL17), 5.0 PK4 (BL17), 5.0, 5.1a, 5.1 PK4 (BL18), 5.1 PK3 (BL17), 5.1	Tru64 Kernel Race Condition	High	CyberNotes-2002-03

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Computalynx ³⁵⁶	Windows 95/98/NT 4.0	CMail 2.4, 2.4.7, 2.4.12 AV, 2.4.12	CMail POP3 Denial Of Service	Low	CyberNotes-2002-18
Computer Associates ³⁵⁷	Unix	CA-MLink	CA-MLink Buffer Overflows	High	CyberNotes-2002-08
Computer Associates ³⁵⁸	Windows NT	eTrust Antivirus EE 6.0	eTrust Antivirus EE Privilege Escalation	High	CyberNotes-2002-25
Computer Associates ³⁵⁹	Unix	InoculateIT 6.0	InoculateIT Incremental Scan Option	Medium	CyberNotes-2002-25
Conectiva ³⁶⁰	Unix	Linux 5.0, 5.1, 6.0	Linux MySQL Implementation	Medium	CyberNotes-2002-02
Cool Forum ³⁶¹	Unix	CoolForum 0.5 beta	CoolForum Source Disclosure	Medium	CyberNotes-2002-21
Coolsoft ³⁶²	Windows 94/98/ME/NT 4.0/2000, XP	PowerFTP 2.10 and prior	PowerFTP Multiple Vulnerabilities	Low/ Medium (Low for the DoS vulnerability; and Medium if sensitive information or elevated privileges are obtained)	CyberNotes-2002-04
Coolsoft ³⁶³	Windows 95/98/ME/ NT 4.0/2000, XP	PowerFTP 2.0 3, 2.10, 2.23, 2.24	PowerFTP Server Remote Denial of Service	Low	CyberNotes-2002-21
Coxco Support ³⁶⁴	Windows 95/98/ME/ NT 4.0/2000, XP	Midicart ASP, Midicart ASP Maxi, Midicart ASP Plus	Midicart ASP Remote Customer Information Retrieval	Medium	CyberNotes-2002-17
Coxco Support ³⁶⁵	Unix	Midicart PHP, PHP Maxi, Midicart PHP Plus	Midicart Arbitrary File Upload	Medium	CyberNotes-2002-20
Coxco Support ³⁶⁶	Unix	Midicart PHP, PHP Maxi, PHP Plus	Midicart Information Disclosure	Medium	CyberNotes-2002-20
CPAN.org ³⁶⁷	Unix	Gisle Aas Digest::MD5 2.16-2.19	Gisle Aas Digest-MD5 UTF-8 Data Integrity	Medium	CyberNotes-2002-10
Critical Path ³⁶⁸	Unix	InJoin Directory Server 4.0	Critical Path InJoin Directory Server File Disclosure & Cross-Site Scripting	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-10
Curtis Specialty Consulting ³⁶⁹	Windows 2000	IISPop 1.161, 1.181	IISPop Remote Denial of Service	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-24
CVS ³⁷⁰	Multiple	CVS 1.11	CVS Daemon RCS Buffer Overflow	High	CyberNotes-2002-11
CVSup ³⁷¹	Multiple	CVSup-mirror 1.2	CVSup-Mirror Insecure Temporary Files	Low/ Medium (Medium if elevated privileges can be obtained)	CyberNotes-2002-23
Cyberstop ³⁷²	Windows 95/98/NT 4.0/2000	Cyberstop Web Server for Windows 0.1	Cyberstop Web Server Denial of Service and MS-DOS Device Denial of Service	Low	CyberNotes-2002-02
Cyrus ³⁷³	Unix	SASL 2.1.9	Cyrus SASL Library Multiple Buffer Overflow Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-25
Cyrusoft ³⁷⁴	Unix	libSieve 2.1.2	libSieve Header Name Buffer Overflow	High	CyberNotes-2002-25
Cyrusoft ³⁷⁵	Unix	libSieve 2.1.2	libSieve Buffer Overflows	High	CyberNotes-2002-25
Cyrus-Utils ³⁷⁶	Unix	SASL LDAP+MYSQL Auth Patch 1.5.24, 1.5.27	SASL LDAP+ MySQL Authentication Patch	Medium	CyberNotes-2002-07
Daan Systems ³⁷⁷	Windows 95/98/ME/NT 4.0/2000, XP	News Reactor 1.0	NewsReactor Insecure Password	Medium	CyberNotes-2002-02

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
DaCode ³⁷⁸	Multiple	DaCode 1.2.0	DaCode News Message HTML Injection	High	CyberNotes-2002-20
Dan Mueth ^{379, 380, 381}	Unix	Scroll Keeper 0.3, 0.3.1, 0.3.4-0.3.6, 0.3.11	ScrollKeeper Tempfile Symbolic Link CVE Name: CAN-2002-0662	High	CyberNotes-2002-18
Darren Reed ³⁸²	Unix	IPFilter 3.4.25	IPFilter TTL Fingerprinting	Medium	CyberNotes-2002-07
Darren Reed ³⁸³ <i>NetBSD issues advisory³⁸⁴</i>	Unix	IPFilter 3.1.1- 3.1.10, 3.2.1- 3.2.22, 3.3.1- 3.3.22, 3.4.1- 3.4.28	IPFilter FTP Proxy Unauthorized Access	Medium	CyberNotes-2002-22 CyberNotes-2002-23
Data Wizard ³⁸⁵	Windows 95/98/NT 4.0/2000	FtpXQ 2.5	FtpXQ Buffer Overflow	Low	CyberNotes-2002-11
Datalex ³⁸⁶	Multiple	Bookit! Consumer 2.0	Bookit! Consumer Plaintext Password Information	Medium	CyberNotes-2002-12
Datawizard Technologies ³⁸⁷	Windows 95/98/NT 4.0/2000	FtpXQ 2.0, 2.1	FtpXQ Privileged Default Account Permissions	Medium	CyberNotes-2002-01
Dave Lawrence ³⁸⁸	Unix	XTux 2001.06.01	XTux Server Denial of Service	Low	CyberNotes-2002-06
David Harris ³⁸⁹	Windows	Pegasus Mail 4.0 1	Pegasus Mail Message Header Buffer Overflow	Low	CyberNotes-2002-15
DayDream ³⁹⁰	Unix	DayDream BBS 2.9-2.13	DayDream BBS Control Code Multiple Buffer Overflow	High	CyberNotes-2002-01
DB4Web ³⁹¹	Multiple	DB4Web 3.4, 3.6	DB4Web Directory Traversal	Medium	CyberNotes-2002-19
DB4Web ³⁹²	Multiple	DB4Web 3.4, 3.6	DB4Web Connection Proxy	Medium	CyberNotes-2002-19
DC Scripts ³⁹³	Unix	DCForum 5.0, 6.0, 6.21, 2000 1.0	DCForum Predictable Password	Medium	CyberNotes-2002-03
DCP- Portal ³⁹⁴	Multiple	DCP-Portal 3.7, 4.0, 4.1, 4.2	DCP-Portal System Information Path Disclosure	Medium	CyberNotes-2002-04
DCP-Portal ³⁹⁵	Multiple	DCP-Portal 3.7, 4.0, 4.1, 4.2	DCP-Portal Cross Site Scripting	High	CyberNotes-2002-04
Debian ³⁹⁶	Unix	CVS Kit CVS Server 1.10.7	CVS Server Denial Of Service	Low	CyberNotes-2002-05
Debian ³⁹⁷	Unix	Debian Linux 2.2 sparc, powerpc, Linux 2.2 IA-32, Linux 2.2 arm, alpha, Linux 2.2 68k	Debian IN.UUCP Remote Denial of Service	Low	CyberNotes-2002-12
Debian ³⁹⁸	Unix	Internet Message 133.0, 141.0	Debian Internet Message Insecure Temporary File Creation	Medium	CyberNotes-2002-25
Debian / RedHat ³⁹⁹	Unix	Interchange 4.8.1-4.8.5	Interchange Arbitrary File Read	Medium	CyberNotes-2002-17
DEC fingerD ⁴⁰⁰	Multiple	DEC fingerD 0.7	DEC FingerD Format String	High	CyberNotes-2002-13
Deep Forest Software ⁴⁰¹	Windows 95/98/NT 4.0/2000	Quik-Serv Webserver 1.1 B	Quik-Serv Web Server Arbitrary File Disclosure	Medium	CyberNotes-2002-07
Deep Metrix ⁴⁰²	Windows	LiveStats 6.2	LiveStats Script Injection	High	CyberNotes-2002-13
Deerfield ⁴⁰³	Windows 95/98/ME/NT 4.0/2000, XP	MDaemon 5.0.0-5.0.5, MDAemon Pro 5.0	MDaemon Multiple Vulnerabilities	Medium	CyberNotes-2002-10
Deerfield ⁴⁰⁴	Windows 95/98/ME/NT 4.0/2000, XP	WorldClient 5.0-5.0.5, Pro 5.0	WorldClient Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-10
Deerfield ⁴⁰⁵	Windows NT	VisNetic Website 3.5.13 .1	Deerfield VisNetic Website OPTIONS Memory Corruption	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-25
Deerfield.com ⁴⁰⁶	Windows NT	WebSite Pro 3.1.11.0	WebSite Pro Filename Request	Medium	CyberNotes-2002-11
DeleGate ⁴⁰⁷	Windows 95/98/ME/NT 4.0/2000, Unix	DeleGate 7.7.0, 7.7.1	DeleGate Cross-Site Scripting	High	CyberNotes-2002-01

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
DeleGate ⁴⁰⁸	Windows NT 4.0/2000, Unix	DeleGate 7.7.0, 7.7.1, 7.8.0, 7.8.1	DeleGate Multiple Buffer Overflow Vulnerabilities	High	CyberNotes-2002-03
Delta Scripts ⁴⁰⁹	Multiple	PHP Classifieds 6.0.5	PHP Classifieds Cross-Site Scripting	High	CyberNotes-2002-13
Demarc Security ⁴¹⁰	Windows NT 4.0/2000, XP, Unix	PureSecure 1.0.5 Windows, 1.0.5 Unix	PureSecure Authentication Bypass	High	CyberNotes-2002-08
Desiderata Software ⁴¹¹	Multiple	Blazix 1.2, 1.2.1	Blazix Special Character Handling	Medium	CyberNotes-2002-18
Digital ⁴¹²	Unix	Digital OSF/1 3.0, 3.0B, 3.2G, 3.2F, 3.2, 3.2 DE1&2, 3.2B-3.2D, UNIX 3.0, 3.2 G	Tru64 UUCP Local Buffer Overflow	High	CyberNotes-2002-19
Digital ⁴¹³	Unix	OSF/1 3.0, 3.0 B, 3.2G, 3.2F, 3.2 DE1&2, 3.2, 3.2 B-D, 4.0, Ultrix 3.0	Tru64 Inc Local Buffer Overflow CVE Name: CAN-2002-1128	High	CyberNotes-2002-19
disipoll ⁴¹⁴	Multiple	disipoll 0.9	disipoll Cookie Security Bypass	Medium	CyberNotes-2002-09
D-Link ⁴¹⁵	Multiple	DWL-1000AP Firmware 3.2.28 #483	DWL-1000AP Wireless LAN Access Point Plaintext Password & Public Community	Medium	CyberNotes-2002-01.
D-Link ⁴¹⁶	Multiple	DP-303	D-Link Denial of Service	Low	CyberNotes-2002-16
D-Link ⁴¹⁷	Multiple	DSL-500	DSL-500 Default Telnet Password	Medium	CyberNotes-2002-22
D-Link⁴¹⁸ <i>Patch now available⁴¹⁹</i>	Multiple	DWL-900AP+ 2.1, 2.2	DWL-900AP+ TFTP Server	Medium/High (High if administrative access can be obtained)	CyberNotes-2002-22 CyberNotes-2002-23
dnrd ⁴²⁰	Unix	dnrd 1.0-2.10	DNRD Bounds Checking Denial of Service	Low	CyberNotes-2002-02
DNSTools Software ⁴²¹	Unix	DNSTools 2.0 Beta 4, 2.0 Beta 3	DNSTools Authentication Bypass	High	CyberNotes-2002-09
Dotmarketing.org ⁴²²	Unix	DotProject 0.2.1 .5	DotProject Authentication Bypass	High	CyberNotes-2002-16
Double Precision Incorporated ⁴²³	Unix	Courier MTA 0.38.1	Courier MTA Remote Denial of Service	Low	CyberNotes-2002-12
Double Precision Incorporated ^{424, 425}	Unix	Courier MTA 0.37.3, 0.40	Courier SqWebMail File Disclosure	Medium	CyberNotes-2002-24
DPGS ⁴²⁶	Multiple	Duma Photo Gallery System 0.99.4	DPGS Form Field Input Validation	Medium	CyberNotes-2002-13
Drupal ⁴²⁷	Unix	Drupal 4.0.0	Drupal News Message HTML Injection	High	CyberNotes-2002-20
Dug Song ⁴²⁸	Multiple	Dsniff 2.3; Fragroute 1.2; Fragrouter 1.6	Fragroute/ Dsniff/ Fragrouter Configure Script Trojan Horse	High	CyberNotes-2002-12
Dug Song ⁴²⁹	Unix	Fragrouter 1.7	Fragrouter Trojan Horse	High	CyberNotes-2002-22
Dynamic Guestbook ⁴³⁰	Unix	Dynamic Guestbook 3.0	Dynamic Guestbook Cross-Site Scripting & Arbitrary Command Execution	High	CyberNotes-2002-07
Ecartis/ Listar ⁴³¹	Unix	Ecartis Ecartis 1.0.0 snapshot 20020125, 20020121; Listar Listar 0.126a, 0.127a, 0.129a	Ecartis/Listar Multiple Buffer Overflow	High	CyberNotes-2002-06
ECS ⁴³²	Multiple	K7S5A(L) V.02/02/06	K7S5A Boot Menu Access	Medium	CyberNotes-2002-11
eDonkey 2000 ⁴³³	Windows	Client 35.16.59 Windows, 35.16.60 Windows	eDonkey 2000 Buffer Overflow	High	CyberNotes-2002-12
EFax ⁴³⁴	Unix	efax 0.8a, 0.9a, 0.9	EFax UUCP Buffer Overflow and '-d' Command Line File Reading	High	CyberNotes-2002-02
Ehud Gavron ⁴³⁵	Unix	TrACESroute 6.0, 6.1, 6.1.1	TrACESroute Terminator Function Format String	High	CyberNotes-2002-12
Ehud Gavron ⁴³⁶	Unix	TrACESroute 6.0, 6.1.1	Traceroute-nanog Buffer Overflow	High	CyberNotes-2002-23

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Ehud Gavron ⁴³⁷	Unix	TrACES route 6.0, 6.1, 6.1.1	Traceroute-Nanog Buffer Overflow Vulnerabilities	High	CyberNotes-2002-24
Ekilat LLC ⁴³⁸	Multiple	php (Reactor) 1.2.7 pl1	PHPReactor HTML Injection	High	CyberNotes-2002-18
Ekilat LLC ⁴³⁹	Unix	php (Reactor) 1.2.7 pl1	PHPReactor Browse.PHP Cross-Site Scripting	High	CyberNotes-2002-21
ELSA ⁴⁴⁰	Multiple	Lancom 1100 Office	Lancom 1100 Office Insecure Web Administration	Medium	CyberNotes-2002-01
EMUMail, Inc. ⁴⁴¹	Unix	EMUMail 3.0; EMUMail for Red Hat Linux 5.0, 5.1; EMUMail for Unix 5.1	EMUMail Arbitrary File Reading	Medium	CyberNotes-2002-08
EMUMail, Inc. ⁴⁴²	Unix	EMUMail 3.0; EMUMail for Red Hat Linux 5.0, 5.1; EMUMail for Unix 5.0, 5.1	EMUMail HTTP Host Arbitrary Config File Loading	High	CyberNotes-2002-08
EMUMail, Inc. ⁴⁴³	Windows, Unix	EMUMail for Red Hat Linux 5.0, EMUMail for Unix 5.0, EMUMail for Windows 5.0	EMUMail Cross-Site Scripting	High	CyberNotes-2002-20
EMUMail, Inc. ⁴⁴⁴	Windows, Unix	EMUMail for Red Hat Linux 5.0, EMUMail for Unix 5.0, EMUMail for Windows 5.0	EMUMail Web Root Path Disclosure	Medium	CyberNotes-2002-20
Endity.com ⁴⁴⁵	Multiple	ShoutBox 1.2	ShoutBox HTML Injection	High	CyberNotes-2002-16
Endymion ⁴⁴⁶	Unix	MailMan WebMail 3.0, 3.0.1, 3.0.4, 3.0.6-3.0.8, 3.0.10- 3.0.16, 3.0.18- 3.0.35	MailMan Sensitive Information	Medium	CyberNotes-2002-05
Enlightenment ⁴⁴⁷	Unix	IMlib2 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4	IMLib2 '\$Home' Environment Variable Buffer Overflow	High	CyberNotes-2002-02
Ensim ⁴⁴⁸	Multiple	Web ppliance 3.0, 3.1	Webpliance Unauthorized E-mail Access	Medium	CyberNotes-2002-16
Enterasys ⁴⁴⁹	Multiple	Smart Switch SSR8000 E8.3.0.4, SSR8000 E8.2.0.0	SSR8000 SmartSwitch Remote Denial of Service	Low	CyberNotes-2002-19
Entercept Security Technologies ⁴⁵⁰	Windows NT 4.0/2000, XP, Unix	Entercept Agent 2.5_win32	Entercept Agent Password Disclosure	Medium	CyberNotes-2002-15
Epic Games ⁴⁵¹	Multiple	Unreal Tournament Server 436.0	Unreal Tournament Server Remote Denial of Service	Low	CyberNotes-2002-14
Eric PrevotEAU ⁴⁵²	Unix	DCTC 0.83.3	DCTC NULL Byte Denial of Service	Low	CyberNotes-2002-20
Eric Raymond ⁴⁵³	Unix	bogofilter 0.9 .0.4	Bogofilter Insecure Temporary File Creation	Medium	CyberNotes-2002-25
Eric Raymond ^{454, 455}	Unix	Fetchmail 5.8.16, 5.8.17, 5.9.1-5.9.9	Fetchmail Message Count Buffer Overflow CVE Name: CAN-2002-0146	Medium	CyberNotes-2002-11
Eric Raymond ^{456, 457, 458}	Unix	Fetchmail 5.4, 5.6-5.8, 5.9.6-5.9.14, 6.0.0	Fetchmail Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Eryq ⁴⁵⁹	Unix	MIME:: Tools 5.4.11	MIME::Tools RFC Parameter Value Continuation	Medium	CyberNotes-2002-12
EServ ⁴⁶⁰	Windows 95/98/NT 4.0	EServ 2.92-2.97	EServ Password Restriction	High	CyberNotes-2002-02
Eshare Communications Incorporated ⁴⁶¹	Windows NT 4.0/2000	Eshare Expressions 1.0, 2.0	Eshare Expressions Directory Traversal	Medium	CyberNotes-2002-03
Essen ⁴⁶²	Windows 95/98/NT 4.0/2000, XP	Essentia Web Server 2.1	Essentia Web Server Denial of Service & Directory Traversal	Low/ Medium (Medium for the Directory Traversal vulnerability)	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Ethereal ⁴⁶³	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Ethereal 0.9.3 & prior	Ethereal Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-11
Ethereal Group ⁴⁶⁴	Windows 95/98/ME/NT 4.0, Unix	Ethereal 0.9.1, 0.9.2	Ethereal ASN.1 Denial of Service	Low	CyberNotes-2002-09
Ethereal Group ^{465, 466}	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Ethereal 0.8.18, 0.9.0-0.9.4	Ethereal Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-14
Ethereal Group ^{467, 468, 469, 470}	Windows 95/98/ME/ NT/ 4.0/2000, XP, Unix	Ethereal 0.9.0-0.9.5	Ethereal ISIS Dissector Memory Corruption	High	CyberNotes-2002-18
Etnus ⁴⁷¹	Unix	TotalView 5.0 .0-4	TotalView Insecure UID/GID Privilege	Medium/High (High if root compromise)	CyberNotes-2002-07
Ettercap ⁴⁷²	Unix	Ettercap 0.6.3.1	Ettercap Buffer Overflow	High	CyberNotes-2002-04
Etype ⁴⁷³	Windows 95/98/NT 4.0/2000, XP	Eserv 2.97	EServ Multiple Vulnerabilities	Low	CyberNotes-2002-03
Evolvable Corporation ⁴⁷⁴	Windows 95/98/NT 4.0/2000	Shambala Server 4.5	Shambala Server FTP Server Directory Traversal & Denial of Service	Low/ Medium (Medium if sensitive information can be obtained)	CyberNotes-2002-12
eZ Systems ⁴⁷⁵	Multiple	HTTP Bench 1.1	HTTPBench Information Disclosure	Medium	CyberNotes-2002-23
EZNE.net ⁴⁷⁶	Unix	Ezboard 1.27	Ezboard Remote Buffer Overflow	High	CyberNotes-2002-04
e-Zone Media Inc. ⁴⁷⁷	Multiple	FuseTalk 2.0, 3.0	FuseTalk Cross-Site Scripting	High	CyberNotes-2002-15
Facto System ⁴⁷⁸	Windows	Weblog 0.9b, 1.0 Beta, 1.1 Beta	Weblog Multiple SQL Injection	High	CyberNotes-2002-18
Fake Ident ⁴⁷⁹	Unix	Fake Identd 0.9 b, 0.9, 1.1-1.4	Fake Identd Client Query Remote Buffer Overflow	High	CyberNotes-2002-16
FAQ Manager ⁴⁸⁰	Unix	FAQ Manager.cgi 2.0-2.2.5	FAQManager.CGI NULL Character Arbitrary File Disclosure	Medium	CyberNotes-2002-01
FAQ Manager ⁴⁸¹	Windows, Unix	FAQ Manager.cgi 2.0-2.2.6	FAQManager.CGI Directory Traversal	Medium	CyberNotes-2002-01
FAQ-O-Matic ⁴⁸²	Unix	FAQ-O-Matic 2.711, 2.712	FAQ-O-Matic Cross-Site Scripting	High	CyberNotes-2002-03
Fastlink Software ⁴⁸³	Multiple	TheServer 1.75	TheServer Plain Text Password Storage	Medium	CyberNotes-2002-15
FileZilla ⁴⁸⁴	Multiple	FileZilla Server 0.7.0	FileZilla Directory Traversal	Medium	CyberNotes-2002-11
Finjan Software ⁴⁸⁵	Windows NT 4.0/2000	SurfinGate 6.0, 6.0 1	SurfinGate URL Filter Bypassing	Medium	CyberNotes-2002-18
FlashFXP ⁴⁸⁶	Windows	FlashFXP 1.4	FlashFXP Password Disclosure	Medium	CyberNotes-2002-22
Floosietek ⁴⁸⁷	Windows NT	FTGate Office 1.0 5, FTGatePro 1.0 5	FTGate Multiple Vulnerabilities	Low/ High (High if arbitrary code can be executed)	CyberNotes-2002-07
Fortres Grand Corporation ⁴⁸⁸	Windows 95/98/ME/ NT 4.0/2000, XP	Fortres 101 4.1	Fortres 101 Software Disabling Protection Circumventing	Medium	CyberNotes-2002-25
Foundry Networks ⁴⁸⁹	Multiple	EdgeIron 4802F 0.0	EdgeIron SNMP Configuration Sensitive Information	Medium	CyberNotes-2002-06

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Foundry Networks ⁴⁹⁰	Multiple	ServerIron 5.1.10t12, 6.0, 7.1.09, ServerIron400 0.0, ServerIron800 0.0, ServerIron XL 0.0, XL/G 0.0	ServerIron URL Decode	Medium	CyberNotes-2002-06
Foundstone ⁴⁹¹	Windows 98/ME/NT 4.0/2000	FScan 1.12	FScan Banner Format String	High	CyberNotes-2002-09
Francisco Burzi ⁴⁹²	Multiple	PHP-Nuke 1.0, 2.5, 3.0, 4.0, 4.3, 4.4, 4.4.1a, 5.0, 5.0.1, 5.1, 5.2a, 5.2, 5.3.1	PHP-Nuke Input Validation	High	CyberNotes-2002-02
Francisco Burzi ⁴⁹³	Multiple	PHP-Nuke 1.0, 2.5, 3.0, 4.0, 4.3, 4.4, 4.4.1a, 5.0, 5.0.1, 5.1, 5.2a, 5.2, 5.3.1, 5.4	PHPNuke Debug Information Disclosure	Medium	CyberNotes-2002-02
Francisco Burzi ⁴⁹⁴	Unix	PHP-Nuke 5.0-5.4	PHP-Nuke Path Disclosure	Medium	CyberNotes-2002-06
Francisco Burzi ⁴⁹⁵	Unix	PHP-Nuke 5.0-5.4, PostNuke 0.62-0.64, 0.7, 0.70	PHP-Nuke Account Hijacking	Medium/High (High if administrative privileges are obtained)	CyberNotes-2002-06
Francisco Burzi ⁴⁹⁶	Unix	PHP-Nuke 6.0	PHPNuke Cross-Site Scripting	Medium	CyberNotes-2002-20
Francisco Burzi ⁴⁹⁷	Windows, Unix	PHP-Nuke 6.0	PHPNuke News Message HTML Injection	High	CyberNotes-2002-20
Francisco Burzi ⁴⁹⁸	Windows, Unix	PHP-Nuke 6.0	PHPNuke Modules.PHP SQL Injection	Low/ Medium (Medium if the database is corrupted)	CyberNotes-2002-20
Francisco Burzi ⁴⁹⁹	Windows, Unix	PHP-Nuke 6.0	PHPNuke Multiple Cross-Site Scripting	High	CyberNotes-2002-21
Francisco Burzi ⁵⁰⁰	Unix	PHP-Nuke 5.6	PHP-Nuke 5.6 SQL Injection CVE Name: CAN-2002-1242	Medium	CyberNotes-2002-23
Francisco Burzi ⁵⁰¹	Multiple	PHP-Nuke 5.0, 5.0.1, 5.1, 5.2 a, 5.2, 5.3.1, 5.4-5.6, 6.0, 6.5 BETA 1	PHP-Nuke Multiple Cross-Site Scripting	High	CyberNotes-2002-24
Francisco Burzi/ Post Nuke Development Team ⁵⁰²	Unix	PHP-Nuke 5.0-5.6; PostNuke Development Team PostNuke 0.62-0.64, 0.70, 0.71, 0.703	PHP-Nuke Cross-Site Scripting	High	CyberNotes-2002-17
Frank McIngvale ^{503, 504}	Unix	LuxMan 0.41	LuxMan File Path CVE Name: CAN-2002-1245	High	CyberNotes-2002-23
Frederic Tyndiuk ⁵⁰⁵	Unix	Eupload 1.0	Eupload Plain Text Password Storage	Medium	CyberNotes-2002-16
Free Peers, Inc. ⁵⁰⁶	Windows 95/98/ME/ NT 4.0/2000, XP	BearShare 2.2-2.2.3, 4.0-4.0.2, 4.0.4-4.0.6	BearShare Directory Traversal	Medium	CyberNotes-2002-21
FreeBSD ⁵⁰⁷	Unix	FreeBSD 4.2-4.4	FreeBSD Package Add Insecure Temporary Directory Creation	Medium	CyberNotes-2002-01
FreeBSD ⁵⁰⁸	Unix	FreeBSD 4.x Heimdal Port 0.4e, 5.x Heimdal Port 0.4e, FreeBSD 4.0-4.4; KTH Heimdal 0.4e	Kerberos 'getlogin()' Function	High	CyberNotes-2002-02
FreeBSD ⁵⁰⁹	Unix	FreeBSD 4.1, 4.1.1, 4.2-4.5	FreeBSD FStatFS Syscall Race Condition	Low	CyberNotes-2002-03
FreeBSD ⁵¹⁰	Unix	FreeBSD 4.5 -STABLE, 4.5-RELEASE	FreeBSD 4.5 syncache / syncookies Denial of Service	Low	CyberNotes-2002-08
FreeBSD ⁵¹¹	Unix	FreeBSD 4.5 -STABLE, 4.5-RELEASE	FreeBSD \ ICMP Echo Reply Denial of Service	Low	CyberNotes-2002-08
FreeBSD ⁵¹²	Unix	FreeBSD 4.3-4.5	FreeBSD Process Information Bypass	Medium	CyberNotes-2002-11
FreeBSD ⁵¹³	Unix	FreeBSD 4.4, 4.5	FreeBSD k5su Utility Membership Validation	Medium/High (High if root access is obtained)	CyberNotes-2002-11
FreeBSD ⁵¹⁴	Unix	FreeBSD 4.5 RELEASE	FreeBSD Accept Filter Remote Denial of Service	Low	CyberNotes-2002-11

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
FreeBSD ⁵¹⁵	Unix	FreeBSD 4.5 STABLE, RELEASE	FreeBSD 'rc' Script Directory Deletion	Medium	CyberNotes-2002-11
FreeBSD ⁵¹⁶	Unix	FreeBSD 4.0-4.6, 4.1.1 – 4.6 STABLE 4.1.1 – 4.3 RELEASE, 4.5-4.6 RELEASE, 4.3 – 4.4 RELENG	FreeBSD Arbitrary FFS Filesystem	High	CyberNotes-2002-16
FreeBSD ⁵¹⁷	Unix	FreeBSD 4.0-4.6, 4.1.1 – 4.6 STABLE 4.1.1 – 4.3 RELEASE, 4.5-4.6 RELEASE, 4.3 – 4.4 RELENG	FreeBSD NFS Denial of Service	Low	CyberNotes-2002-16
FreeBSD ⁵¹⁸	Unix	FreeBSD 4.3 –RELEASE, 4.4 – STABLE, 4.4 –RELENG, 4.4, 4.5 –STABLE, 4.5 –RELEASE, 4.5, 4.6 –STABLE, 4.6 –RELEASE, 4.6	FreeBSD kqueue Denial of Service	Low	CyberNotes-2002-16
FreeBSD ⁵¹⁹	Unix	FreeBSD 4.0-4.6, 4.1.1-4.5-Stable, 4.1.1–4.3-Release, 4.5-4.6-Release	FreeBSD Signed Integer Buffer Overflow	Medium	CyberNotes-2002-17
FreeBSD ⁵²⁰	Unix	AIDE Port 0.7_1	FreeBSD AIDE Port Default Configuration File	Medium	CyberNotes-2002-18
FreeBSD ^{521,522}	Unix	FreeBSD 4.2-4.6	FreeBSD Ports libkvm Vulnerabilities	High	CyberNotes-2002-19
FreeNews ⁵²³	Unix	FreeNews 2.1	FreeNews Remote Command Execution	High	CyberNotes-2002-24
FreeWnn ⁵²⁴	Unix	FreeWnn 1.1	FreeWnn Jserver Input	High	CyberNotes-2002-02
Funsoft ⁵²⁵	Windows 95/98/ME	Dino's Webserver 1.0, 1.2	Dino's Webserver Directory Traversal	Medium	CyberNotes-2002-02
Funsoft ⁵²⁶	Windows 95/98/ME	Dino's Webserver 1.0, 1.2	Dino's Webserver Denial of Service	Low	CyberNotes-2002-04
Funsoft ⁵²⁷	Windows 95/98/ME	Dino's Webserver 1.2	Dino's Webserver File Disclosure CVE Name: CAN-2002-1133	Medium	CyberNotes-2002-20
Gabriele Bartolini ⁵²⁸	Unix	ht://Check 1.1	ht://Check Web Header Cross-Site Scripting	High	CyberNotes-2002-19
Gafware ⁵²⁹	Windows	CFXImage 1.6.4, 1.6.6	CFXImage 'Show Temp.cfm' File Disclosure	Medium	CyberNotes-2002-11
Galacticomm Technologies ⁵³⁰	Windows	Worldgroup Enterprise Edition 3.20, LITE Personal Server 3.20	Worldgroup Remote FTP Denial of Service	Low	CyberNotes-2002-05
Game Cheats ⁵³¹	Windows	Advanced Web Server Professional 1.0.3 0000	Advanced Web Server Remote Denial of Service	Low	CyberNotes-2002-13
Gateway ⁵³²	Unix	GS-400	GS-400 Server Default Administrator Password	High	CyberNotes-2002-17
Gator ⁵³³	Windows	Gator 3.0.6.0	Gator Insecure Plugin	High	CyberNotes-2002-04
GazTek ⁵³⁴	Unix	ghttpd 1.4-1.4.3	ghttpd Log() Buffer Overflow	High	CyberNotes-2002-21
GDAM ⁵³⁵	Unix	GDAM 0.933, 0.942	GDAM123 Filename Buffer Overflow	High	CyberNotes-2002-18
Geeklog ⁵³⁶	Windows NT 4.0/2000, Unix	Geeklog 1.3	Geeklog New User Default Admin Privileges	High	CyberNotes-2002-01
Geeklog ⁵³⁷	Unix	Geeklog 1.3	Geeklog Permanent Cookie Authentication	High	CyberNotes-2002-02
Geeklog ⁵³⁸	Multiple	Geeklog 1.3.5	Geeklog Multiple Vulnerabilities	High	CyberNotes-2002-12
Geeklog ⁵³⁹	Unix	Geeklog 1.3.5, 1.3.5 sr1	Geeklog Cross-Site Scripting & Send Email Facility	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-15
Ghost View ⁵⁴⁰ <i>Patches are released^{541, 542, 543, 544, 545, 546, 547, 548}</i> <i>More patches released^{549, 550}</i>	Unix	GhostView 1.3, 1.4, 1.4.1, 1.5, gv 2.7 b1-b5, 2.7.6, 2.9.4, 3.0.0, 3.0.4, 3.1.4, 3.1.6, 3.2.4, 3.4.2, 3.4.3, 3.4.12, 3.5.2, 3.5.3, 3.5.8	GhostView Buffer Overflow CVE Name: CAN-2002-0838	High	CyberNotes-2002-20 CyberNotes-2002-22 CyberNotes-2002-24

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
GhostView ^{551, 552}	Unix	GhostView 1.3, 1.4, 1.4.1, 1.5; gv 2.7 b1-b5, 2.7.6, 2.9.4, 3.0.0, 3.0.4, 3.1.4, 3.1.6, 3.2.4, 3.4.2, 3.4.3, 3.4.12, 3.5.2, 3.5.3, 3.5.8	GhostView GZip Command Execution	High	CyberNotes-2002-20
Global Sun Technology, Inc. ⁵⁵³	Multiple	D-Link DWL-900AP+ 2.2; GlobalSunTech WISECOM GL2422AP-0T; Linksys WAP11 2.2	GlobalSunTech Access Point Information Disclosure	Medium	CyberNotes-2002-23
GNU ⁵⁵⁴	Unix	Chess 5.02	Chess Command Buffer Overflow	High	CyberNotes-2002-02
GNU ⁵⁵⁵	Unix	groff 1.10, 1.11a, 1.11, 1.14-1.17	Groff Buffer Overflow CVE Name: CAN-2002-0003	High	CyberNotes-2002-02
GNU ⁵⁵⁶ <i>Vendors release patches^{557, 558}</i>	Unix	Fileutils 4.0, 4.1, 4.1.6	Fileutils Race Condition	Medium	CyberNotes-2002-06 CyberNotes-2002-11
GNU ⁵⁵⁹	Unix	screen 3.9.4, 3.9.8-3.9.11	Screen Braille Module Buffer Overflow	High	CyberNotes-2002-09
GNU ⁵⁶⁰ <i>More patches released⁵⁶¹</i>	Unix	SharUtils 4.2; Caldera OpenLinux Server 3.1, 3.1.1, OpenLinux Workstation 3.1, 3.1.1	SharUtils UUDecode Symbolic Link Attack CVE Name: CAN-2002-0178	Medium	CyberNotes-2002-10 CyberNotes-2002-22
GNU ⁵⁶²	Unix	Mailman 2.0.1- 2.0.10	Mailman Pipemail HTML Injection	High	CyberNotes-2002-11
GNU ⁵⁶³	Unix	Mailman 2.0-2.0.10	Mailman Cross-Site Scripting	High	CyberNotes-2002-11
GNU ⁵⁶⁴	Unix	Mailman 2.0-2.0.11	GNU Mailman Subscribe & Admin Login Cross-Site Scripting Vulnerabilities	High	CyberNotes-2002-15
GNU ^{565, 566}	Unix	Enscript 1.4-1.6.1	Enscript Insecure Temporary File Function	Medium	CyberNotes-2002-02
GNU ^{567, 568, 569}	Unix	tar 1.13.25	GNU Tar Archive Files CVE Name: CAN-2002-0399	Medium	CyberNotes-2002-20
GNU ^{570, 571, 572}	Unix	wget 1.5.3, 1.6, 1.7, 1.7.1, 1.8, 1.8.1, 1.8.2	WGet NLST Client Side File Overwriting CVE Name: CAN-2002-1344	Medium	CyberNotes-2002-25
GNU/ Pipemail ⁵⁷³	Unix	GNU Mailman 1.0, 2.0 beta3-beta5, 2.0.5-2.0.8, 2.0-2.0.3, 2.0.4, 2.0.9, 2.0.10, 2.1 b1; Pipemail 0.05	Pipemail/ Mailman Insecure Permissions	Medium	CyberNotes-2002-09
GNUJSP ⁵⁷⁴	Windows NT 4.0/2000, Unix	GNUJSP 1.0.0, 1.0.1	GNUJSP File Disclosure	Medium	CyberNotes-2002-04
gnuplot ⁵⁷⁵	Unix	gnuplot 3.7	GNUPlot French Documentation Buffer Overflow	High	CyberNotes-2002-25
GoAhead Software ⁵⁷⁶	Windows 95/98/ME/NT 4.0, Unix	GoAhead WebServer 2.1, (Windows) 2.1	GoAhead WebServer Cross-Site Scripting & Directory Traversal	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-14
GoAhead Software ⁵⁷⁷	Windows 95/98/NT 4.0, Unix	GoAhead WebServer 2.1	GoAhead WebServer Buffer Overflow	High	CyberNotes-2002-17
Google ⁵⁷⁸	Multiple	Toolbar 1.1.41- 1.1.45, 1.1.47-1.1.49, 1.1.53- 1.1.58	Google Toolbar Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-16
Google ⁵⁷⁹	Multiple	Google Toolbar 1.1.60	Google Toolbar Denial of Service	Low	CyberNotes-2002-17
Gordano ⁵⁸⁰	Windows NT 4.0/2000, XP	NTMail 8.0	NTMail JUCE E-mail Filter	Low	CyberNotes-2002-24

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Gordano ⁵⁸¹	Windows NT	NTMail 8.0	Gordano Mail Server 'rword' Filter Bypass	Medium	CyberNotes-2002-25
GOST ⁵⁸²	Multiple	34.19-2001 Standard Implementation	34.19-2001 Standard Implementation Key Data Compromise	Medium	CyberNotes-2002-13
GPM ⁵⁸³	Unix	GPM 1.17.8	GPM-Root Format String	High	CyberNotes-2002-01
GR Security ⁵⁸⁴	Unix	GRSecurity Kernel Patch 1.9.4	GRSecurity Linux Kernel Memory Protection	Medium	CyberNotes-2002-11
Gravity Storm Software ⁵⁸⁵	Windows NT 4.0/2000, XP	Service Pack Manager 2000 6.0, 6.1, 6.3	Service Pack Manager 2000 Directory Permissions	Medium	CyberNotes-2002-07
Gregory Trubetskoy ^{586, 587}	Unix	mod_python 2.7-2.7.7	mod_python Imported Module Access CVE Name: CAN-2002-0185	Medium	CyberNotes-2002-09
GRSecurity ⁵⁸⁸	Unix	GRSecurity Kernel Patch 1.9.4	GRSecurity Linux Kernel Memory Protection	Medium	CyberNotes-2002-10
GTetrinet ⁵⁸⁹	Multiple	GTetrinet 0.4-0.4.3	GTetrinet Multiple Remote Buffer Overflow Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-22
GTetrinet ⁵⁹⁰	Unix	GTetrinet 0.4-0.4.3	GTetrinet Multiple Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-25
Hans Persson ⁵⁹¹	Unix	Molly 0.5	Molly Host Execute Commands	High	CyberNotes-2002-22
Hanterm ⁵⁹²	Unix	Hanterm 3.3	Hanterm Buffer Overflow	High	CyberNotes-2002-03
Harald Hoyer ⁵⁹³	Unix	Autorun 2.7	Autorun Arbitrary File Read	Medium	CyberNotes-2002-11
Hardcore Software ⁵⁹⁴	Unix	Anti-Web HTTPD 2.2	Anti-Web HTTPD Script Engine File Opening Denial Of Service	Low	CyberNotes-2002-01
Hardcore Software ⁵⁹⁵	Unix	Anti-Web HTTPD 2.2	Anti-Web HTTPD Script Engine Heap Overflow	High	CyberNotes-2002-01
Hewlett Packard Systems ⁵⁹⁶	Unix	HP-UX 10.20 Series 800, Series 700, 11.0, 11.11, HP-UX (VVOS) 11.04	HP-UX mmap() Denial of Service	Low	CyberNotes-2002-01
Hewlett Packard Systems ⁵⁹⁷	Unix	HP-UX 10.20, 11.0, 11.11	HP "Diagnostic- Code" Leakage	Medium	CyberNotes-2002-02
Hewlett Packard Systems ⁵⁹⁸	Multiple	JetDirect x.08.32	JetDirect SNMP Denial of Service	Low	CyberNotes-2002-04
Hewlett Packard Systems ⁵⁹⁹	Unix	HP9000 Series 700/800 running HP-UX releases 10.20 & 11.x	HP-UX Java Applet Browser Traffic Redirect CVE Name: CAN-2002-0058	High	CyberNotes-2002-05
Hewlett Packard Systems ⁶⁰⁰	Multiple	ProCurve Switch 4000M 0.0	ProCurve Switch Denial of Service	Low	CyberNotes-2002-05
Hewlett Packard Systems ⁶⁰¹	Multiple	MPE/iX 6.0, 6.5, 7.0	MPE/iX Denial of Service	Low	CyberNotes-2002-09
Hewlett Packard Systems ⁶⁰²	Multiple	MPE/iX 6.0, 6.5, 7.0	MPE/iX FTPSRVR Arbitrary Shell Command Execution	High	CyberNotes-2002-09
Hewlett Packard Systems ⁶⁰³	Unix	VirtualVault 4.5	VirtualVault Unauthorized Administrative Access	Medium	CyberNotes-2002-10
Hewlett Packard Systems ⁶⁰⁴	Unix	CIFS/9000 Server A.01.06, A.01.05	CIFSLogin Buffer Overflow	High	CyberNotes-2002-13
Hewlett Packard Systems ⁶⁰⁵	Unix	HP-UX 11.0 4, 11.0, 11.11	HP-UX PTrace Denial of Service	Low	CyberNotes-2002-16
Hewlett Packard Systems ⁶⁰⁶	Multiple	JetDirect x.21.00, x.20.00, x.08.32, x.08.20, x.08.05, x.08.04, x.08.00, JetDirect J3111A rev. G.08.03, G.07.17, G.07.03, G.07.02, G.05.35, A.08.06	JetDirect Administrative Password Retrieval	Medium	CyberNotes-2002-16

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Hewlett Packard Systems ⁶⁰⁷	Windows NT 4.0/2000, Unix	OpenView Emanate SNMP Agent 14.2 Win NT/2k, Solaris 2.X, HP-UX 11.X, 10.20	EMANATE 14.2 Predictable SNMP Community String	Low/ Medium (Medium if unauthorized access is obtained)	CyberNotes-2002-16
Hewlett Packard Systems ⁶⁰⁸	Unix	HP Secure OS Software for Linux 1.0	HP Secure OS Software for Linux TLCompAdd MAC Restrictions	Medium	CyberNotes-2002-17
Hewlett Packard Systems ⁶⁰⁹	Unix	HP Secure OS software for Linux 1.0	HP Secure OS For Linux PTrace / IOCTL Unauthorized Access	Medium	CyberNotes-2002-17
Hewlett Packard Systems ⁶¹⁰	Unix	HP-UX (VVOS) 11.0 4	HP-UX VVOS Unspecified Local Password	Medium/High (High if administrative access is obtained)	CyberNotes-2002-17
Hewlett Packard Systems ⁶¹¹	Unix	Virtual Vault 4.0, 4.5, 4.6	Virtual Vault TGA Stack Corruption	Medium/High (High if administrative access is obtained)	CyberNotes-2002-17
Hewlett Packard Systems ⁶¹²	Unix	HP-UX 10.20, 11.0, 11.11	HP-UX LP Subsystem & LP Spool Commands Vulnerabilities	Low	CyberNotes-2002-18
Hewlett Packard Systems ⁶¹³	Unix	HP-UX 11.0	HP-UX VJE.VJE-RUN Default Path Modification	Medium	CyberNotes-2002-18.
Hewlett Packard Systems ⁶¹⁴	Unix	Compaq Tru64 4.0g, 4.0g PK3 (BL17), 4.0f, 4.0 f PK7 (BL18), 4.0 f PK6 (BL17), 5.0a, 5.0 a PK3 (BL17), 5.0, 5.0 PK4 (BL18), 5.0 PK4 (BL17), 5.1a, 5.1a PK2 (BL2), 5.1a PK1 (BL1), 5.1, 5.1 PK5 (BL19), 5.1 PK4 (BL18), 5.1 PK3 (BL17); Digital OSF/1 3.0, 3.0 B, 3.2, 3.2 G, 3.2 F, 3.2 DE1&2, 3.2 B-3.2D	Tru64/OSF1 DXTerm Buffer Overflow CVE Name: CAN-2002-1129	High	CyberNotes-2002-19
Hewlett Packard Systems ⁶¹⁵	Unix	LDAP-UX Integration B.03.00, B.02.00	LDAP-UX Integration Pam-Authz Privilege Elevation	Medium	CyberNotes-2002-20
Hewlett Packard Systems ⁶¹⁶	Unix	Virtual Vault 4.5, 4.6	VirtualVault Apache mod_ssl Remote Denial of Service	Low	CyberNotes-2002-20
Hewlett Packard Systems ⁶¹⁷	Unix	Compaq Tru64 4.0 g PK3 (BL17), 4.0f PK7 (BL18), 5.0a PK3 (BL17), 5.1a PK3 (BL3), 5.1 PK5 (BL19)	HP Tru64 Unspecified Remote Route Daemon	Medium	CyberNotes-2002-21
Hewlett Packard Systems ⁶¹⁸	Unix	OnlineJFS 3.1	HP OnLineJFS Security Measures	Medium	CyberNotes-2002-21
Hewlett Packard Systems ⁶¹⁹	Unix	TruCluster Server 5.0A, 5.1A, 5.1	TruCluster Server Cluster Interconnect Remote Denial of Service CVE Name: CAN-2002-0711	Low	CyberNotes-2002-23
Hewlett Packard Systems ⁶²⁰	Unix	HP-UX 10.20, 10.24, 11.04, 11.0, 11.11	HP-UX xntpd Denial of Service	Low	CyberNotes-2002-25
Hewlett Packard Systems ⁶²¹	Unix	HP-UX 11.0, 11.11	HP-UX Visualize Conference Insecure Default Permissions	Medium	CyberNotes-2002-25
Hewlett Packard Systems ⁶²²	Multiple	Advance Stack 10Base-T Switching Hub J3210A	AdvanceStack Authentication Bypass	High	CyberNotes-2002-04
Hewlett Packard Systems ⁶²³	Unix	HP-UX 11.11	HP-UX 'strlimit()' Denial of Service	Low	CyberNotes-2002-04
Hewlett Packard Systems ⁶²⁴	Multiple	Praesidium Webproxy 1.0	Praesidium Webproxy Unauthorized Access	Medium	CyberNotes-2002-07
Hewlett Packard Systems ⁶²⁵	Mac OS X	Photosmart Print Driver for Mac OS X 1.2.1	Photosmart Mac OS X Print Driver Weak File Permissions	High	CyberNotes-2002-08
Hewlett Packard Systems ⁶²⁶	Unix	HP-UX 11.0, 11.11, HP-UX (VVOS) 11.0 4	HP-UX Password File Corruption	Low	CyberNotes-2002-09

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Hewlett Packard Systems ⁶²⁷	Unix	HP-UX 11.11	HP-UX NDD Denial of Service	Low	CyberNotes-2002-10
Hewlett Packard Systems ⁶²⁸	Unix	Advanced Server/ 9000 B.04.05-B.04.09	Advanced Server/9000 Denial of Service	Low	CyberNotes-2002-14
Hewlett Packard Systems ⁶²⁹	Unix	HP-UX 11.11	HP-UX DCED & RPCD Services Remote Denial of Service	Low	CyberNotes-2002-14
Hewlett Packard Systems ⁶³⁰	Unix	Instant Support Enterprise Edition	HP Instant Support Enterprise Edition Unauthorized File Access	Medium	CyberNotes-2002-15
Hewlett Packard Systems ⁶³¹	Multiple	Business Inkjet 2600, color LaserJet 4550, Designjet 5000, LaserJet 4100, 8150, 9000	JetDirect Embedded Web Server	Low/ Medium (Medium if unauthorized access is obtained)	CyberNotes-2002-16
Hewlett Packard Systems ⁶³²	Multiple	ChaiVM	ChaiVM Arbitrary Service Modification & JAR Signature Validation	Medium	CyberNotes-2002-16
Hewlett Packard Systems ⁶³³	Multiple	ProCurve Switch 4000M	ProCurve Switch Denial of Service	Low	CyberNotes-2002-16
Hewlett Packard Systems ⁶³⁴	Multiple	Procurve Switch 1600M, 2400M, 2424M, 4000M, 8000M	Procurve 4000M Switch Device Reset Denial of Service	Low	CyberNotes-2002-20
Hewlett Packard Systems ⁶³⁵	Unix	Compaq Tru64 4.0g, Tru64 4.0f, HP TruCluster 1.6	Tru64/ TruCluster OSIS V5.4 LDAP Module Unauthorized Access	Medium	CyberNotes-2002-23
Hewlett Packard Systems ⁶³⁶	Unix	HP-UX 10.10, 10.20, 11.0	HP-UX ied Information Disclosure	Medium	CyberNotes-2002-25
Hewlett Packard, Systems ⁶³⁷	Unix	HP-UX 11.0, 11.11	HP-UX SD Data View Denial Of Service	Low	CyberNotes-2002-12
Heysoft ⁶³⁸	Windows NT	EventSave 5.1, 5.2, EventSave+ 5.1, + 5.2	EventSave Event Log Notification	Low	CyberNotes-2002-23
HNS ⁶³⁹	Unix	HNS 2.00-pl0-2.00-pl4, 2.10-pl1, hns-lite 0.6-0.8	HNS Multiple Cross-Site Scripting	High	CyberNotes-2002-04
Horde Project ⁶⁴⁰	Unix	IMP 2.2.7	IMP Cross-Site Scripting & Path Disclosure	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-08
Hosting Controller ⁶⁴¹	Windows NT 4.0/2000	Hosting Controller 1.4.1	Hosting Controller Multiple Vulnerabilities	High	CyberNotes-2002-01
Hosting Controller ⁶⁴²	Windows NT 4.0/2000	Hosting Controller 1.1, 1.3, 1.4b, 1.4, 1.4.1	Hosting Controller Invalid Username	Medium	CyberNotes-2002-03
Hosting Controller ⁶⁴³	Windows NT 4.0/2000	Hosting Controller 1.4, 1.4.1	Hosting Controller Weak Permissions Checking	Medium	CyberNotes-2002-06
Hosting Controller ⁶⁴⁴	Windows NT 4.0/2000	Hosting Controller 1.1, 1.3, 1.4, 1.4b, 1.4.1	Hosting Controller 'Browse.ASP' File Disclosure	Medium	CyberNotes-2002-11
Hosting Controller ⁶⁴⁵	Windows NT 4.0/2000	Hosting Controller 1.1, 1.3, 1.4, 1.4b, 1.4.1	Hosting Controller Default Administrative Account	High	CyberNotes-2002-11
Hosting Controller ⁶⁴⁶	Windows NT 4.0/2000	Hosting Controller 1.1, 1.3, 1.4, 1.4b, 1.4.1	Hosting Controller 'DSNManager' Directory Traversal & Import Root	Medium	CyberNotes-2002-11
Hosting Controller ⁶⁴⁷	Windows NT 4.0/2000	Hosting Controller 1.4, 2002	Hosting Controller Hidden Field Password Changing	Medium	CyberNotes-2002-15
Hotfoon ⁶⁴⁸	Multiple	Hotfoon 4.0	Hotfoon Dialer Plain Text Password Storage & Buffer Overflow	Low/ Medium/High (Medium if unauthorized access can be obtained and High if arbitrary code can be executed)	CyberNotes-2002-23
Hotline Communications ⁶⁴⁹	Windows 95/98/NT 4.0/2000	Hotline Connect 1.8.5	Hotline Connect Plaintext Password	Medium	CyberNotes-2002-05
ht://Dig Group ⁶⁵⁰	Unix	ht://Dig 3.1.5, 3.1.6, 3.2.0	ht://Dig Cross-Site Scripting	High	CyberNotes-2002-13

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Hughes Technologies ⁶⁵¹ <i>Patch now available</i> ⁶⁵²	Unix	LibHTTPD 1.2	LibHTTPD POST Buffer Overflow	High	CyberNotes-2002-23 CyberNotes-2002-24
Hughes Technology ⁶⁵³		Mini SQL 2.0.10- 2.0.13	Hughes Technologies Mini SQL Denial of Service	Low	CyberNotes-2002-01
Hugo Cisneiros ⁶⁵⁴	Multiple	phpSquid Pass 0.11	PHPSquidPass Unauthorized User Deletion	Medium	CyberNotes-2002-13
Hylafax ⁶⁵⁵	Unix	Hylafax 4.0 p12, 4.0 p11, 4.0 p10, 4.0.2, 4.1, 4.1 -beta1-3, 4.1.1, 4.1.2	Hylafax Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-16
IBM ⁶⁵⁶	Multiple	Lotus Domino 5.0.9a	Lotus Domino MS-DOS Device Path Disclosure	Medium	CyberNotes-2002-07
IBM ⁶⁵⁷	Multiple	Informix Web Datablade 4.10-4.12	IBM Informix Web Datablade Page Request SQL Injection	Medium	CyberNotes-2002-08
IBM ⁶⁵⁸	Multiple	Informix Web Datablade 4.10-4.13	Informix Web Datablade SQL Query HTML Decoding	High	CyberNotes-2002-08
IBM ⁶⁵⁹	Multiple	Tivoli Storage Manager 4.2, 4.2.1	Tivoli Storage Manager Buffer Overflow	High	CyberNotes-2002-08
IBM ⁶⁶⁰	Windows NT 4.0/2000	Tivoli Storage Manager 4.2, 4.2.1	Tivoli Storage Manager Client Acceptor Buffer Overflow	High	CyberNotes-2002-08
IBM ⁶⁶¹	Unix	DB2 Universal Database for AIX 6.0, 6.1, 7.0-7.2, DB2 Universal Database for HP-UX 6.0, 6.1, 7.0-7.2, DB2 Universal Database for Linux 6.0, 6.1, 7.0-7.2, DB2 Universal Database for Solaris 6.0, 6.1, 7.0-7.2	DB2 'db2ckpw' Buffer Overflow	High	CyberNotes-2002-11
IBM ⁶⁶²	Unix	Informix SE 7.25.UC1	Informix SE Buffer Overflow	High	CyberNotes-2002-12
IBM ⁶⁶³	Multiple	Tivoli Management Framework 3.6, 3.6.1, 3.7, 3.7.1	Tivoli ManagedNode Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-15
IBM ⁶⁶⁴	Unix	Tivoli Management Framework 3.6, 3.6.1, 3.7, 3.7.1	Tivoli Endpoints Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-15
IBM ⁶⁶⁵	Windows 2000	WebSphere Application Server 4.0.3	WebSphere Large HTTP Header Denial of Service	Low	CyberNotes-2002-19
IBM ⁶⁶⁶	Unix	AIX 4.3, 4.3.1, 4.3.2, 4.3.3, 5.1	IBM AIX ERRPT Buffer Overflow	High	CyberNotes-2002-20
IBM ⁶⁶⁷	Unix	AIX 4.3.3, 5.1	AIX TCP Packet Remote Denial of Service	Low	CyberNotes-2002-21
IBM ⁶⁶⁸	Multiple	SecureWay Firewall 4.2, 4.2.1	SecureWay Firewall Remote Denial of Service	Low/High (High if DoS best practices not in place)	CyberNotes-2002-21
IBM ⁶⁶⁹ <i>Update available</i> ⁶⁷⁰	Multiple	Infoprint Controller Software 1.0 47012	Infoprint Printers Denial of Service	Low	CyberNotes-2002-22 CyberNotes-2002-23
IBM ⁶⁷¹	Windows 2000, Unix	WebSphere Caching Proxy Server 3.6, 4.0	WebSphere Caching Proxy Remote Denial of Service CVE Name: CAN-2002-1169	Low	CyberNotes-2002-22

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
IBM ⁶⁷²	Windows NT 4.0/2000, Unix	WebSphere Caching Proxy Server 3.6, 4.0	IBM Websphere Vulnerabilities CVE Names: CAN-2002-1167, CAN-2002-1168	High	CyberNotes-2002-22
IBM ⁶⁷³	Unix	AIX 4.3.3, 5.1	AIX Selective ACK Denial of Service	Low	CyberNotes-2002-24
IBM ⁶⁷⁴	Multiple	HTTP Server 1.0	IBM HTTP Server Information Disclosure	Medium	CyberNotes-2002-24
Icecast ⁶⁷⁵	Windows 2000, Unix	Icecast 1.3.10, 1.3.7, 1.3.8 beta2, 1.3.11, WIN32 1.3.7	Icecast Buffer Overflow	High	CyberNotes-2002-07
Icecast ⁶⁷⁶	Unix	Icecast 1.3.12	Icecast Server Directory Traversal	Medium	CyberNotes-2002-14
IcrediBB ⁶⁷⁷	Multiple	IcrediBB Beta 1.1	IcrediBB Script Injection	High	CyberNotes-2002-09
id Software ⁶⁷⁸	Multiple	Quake II Server 3.20, Server 3.21	Quake II Server Remote Information Disclosure	Medium	CyberNotes-2002-10
Identix ⁶⁷⁹	Windows NT 4.0/2000, XP	BioLogon 3.0	BioLogon GINA Authentication Bypass	High	CyberNotes-2002-04
IDS ⁶⁸⁰	Multiple	IDS (Image Display System) 0.8.1	Image Display System Directory Disclosure	Medium	CyberNotes-2002-11
Ikonboard.com ⁶⁸¹	Unix	Ikonboard 2.17	Ikonboard Cross-Site Scripting	High	CyberNotes-2002-05
Ikonboard.com ⁶⁸²	Multiple	Ikonboard 2.1.9	Ikonboard Message Body Cross Agent Scripting	High	CyberNotes-2002-09
Ikonboard.com ⁶⁸³	Multiple	Ikonboard 3.0 .1	Ikonboard Flash File	High	CyberNotes-2002-12
Ikonboard.com ⁶⁸⁴	Unix	Ikonboard 3.1.1	Ikonboard User Profile Photo URI HTML Injection	High	CyberNotes-2002-25
Ikonboard.com ⁶⁸⁵	Unix	Ikonboard 3.1.1	Ikonboard X-Forwarded-For: Proxy Header Field HTML Injection	High	CyberNotes-2002-25
Ilia Alshanetsky ⁶⁸⁶	Unix	FUDForum 1.2.8, 1.9.8, 2.0.2	FUDForum Multiple Vulnerabilities	Medium/High (High if arbitrary SQL is executed)	CyberNotes-2002-17
Imatix ⁶⁸⁷	Windows 98/ME	Xitami for Windows 2.5 b5, 2.5 b4	Xitami GSL Template	High	CyberNotes-2002-13
Imatix ⁶⁸⁸	Windows NT	Xitami version 2.5b5	Xitami Connection Flood Denial of Service	Low	CyberNotes-2002-16
IMHO ⁶⁸⁹	Multiple	IMHO Webmail 0.96, 0.96.1-0.96.3, 0.97, 0.97.1, 0.98, 0.98.2, 0.98.3	IMHO Webmail Account Hijacking	Medium	CyberNotes-2002-15
Imlib ⁶⁹⁰	Unix	Imlib 1.9-1.9.12	Imlib Untrusted Images	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-06
Incognito Software Inc. ⁶⁹¹	Multiple	iSMTP Gateway 5.0.1	iSMTP Gateway Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-23
IncrediMail Ltd. ⁶⁹²	Windows 95/98/ME/NT 4.0/2000, XP	IncrediMail 0.0 Build 618, Build 560, Build 1400185	IncrediMail Attachment Location	High	CyberNotes-2002-06
Independent Solution ⁶⁹³	Multiple	Simple Site Searcher, Super Site Searcher	Super Site Searcher Remote Command Execution	High	CyberNotes-2002-18
Infopop ⁶⁹⁴	Unix	Ultimate Bulletin Board 5.4.7e, 5.4.3, 6.0Beta- 6.0.3, 6.0.4f, 6.2.0 Beta Release 1.0	Ultimate Bulletin Board Cross-Site Scripting	High	CyberNotes-2002-01
Infopop ⁶⁹⁵	Windows NT 4.0/2000, Unix	UBBThreads 5.4; Wired Community Software WWW Threads 5.0.9, 5.0.8, 5.0.6, 5.0	UBBThreads/WWWThreads Arbitrary File	High	CyberNotes-2002-03
Info-ZIP ^{696, 697, 698}	Unix	UnZip 5.2, 5.3, 5.31, 5.32, 5.40, 5.42	Info-ZIP UnZip Archive Files CVE Names: CAN-2001-1268, CAN-2001-1269	Medium	CyberNotes-2002-20

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Inktomi ⁶⁹⁹	Unix	Media-IXT 3.0.4, Traffic Edge 1.1.2, 1.5.0, Traffic Server 4.0.18, 4.0.20, 5.1.3, 5.2.0-R, 5.2.1, 5.2.2	Traffic Server Remote Buffer Overflow	High	CyberNotes-2002-14
Inso ⁷⁰⁰	Unix	dwhttpd 4.0.2 a7a, 4.1 a6	DynaWeb httpd Format String	High	CyberNotes-2002-16
Instant Servers ⁷⁰¹	Windows	MiniPortal 1.1.5	MiniPortal Multiple Vulnerabilities	Medium/ High <i>(High if arbitrary code can be executed)</i>	CyberNotes-2002-04
Intel Corporation ⁷⁰²	Multiple	D845BG Motherboard P05-0024, P04-0023, P03-0021, P02-0015, P01-0012, D845HV Motherboard P11-0040, P10-0038, P09-0035, P08-0031, P07-0029, P06-0024, P05-0022, P04-0018, D845PT Motherboard P05-0024, P04-0023, P03-0021, P02-0015, P01-0012, D845WN Motherboard P11-0040, P10-0038, P09-0035, P08-0031, P07-0029, P06-0024, P05-0022, P04-0018	Intel D845 Motherboard BIOS Series Boot Media	Medium	CyberNotes-2002-09
Inter ⁷⁰³	Multiple	qmailadmin 1.0.1, 1.0.2	qmailadmin Buffer Overflow	Medium	CyberNotes-2002-16
Internet Security Systems ⁷⁰⁴ <i>Further research released.</i> ⁷⁰⁵	Windows 2000, XP	BlackIce Agent 3.0, 3.1, BlackIce Defender 2.9caq, 2.9cap; RealSecure Server Sensor 6.0.1 Win, 6.5 Win	BlackIce and RealSecure Denial of Service and Buffer Overflow	Low/High <i>(High if DDoS best practices not in place and arbitrary code can be executed.)</i>	CyberNotes-2002-03 CyberNotes-2002-04
Internet Security Systems ⁷⁰⁶	Multiple	RealSecure for Nokia 6.0	RealSecure for Nokia Default Configuration	High	CyberNotes-2002-06
Internet Security Systems ⁷⁰⁷	Multiple	RealSecure Network Sensor 5.0 XPU 3.4, 5.5 XPU 3.4, 5.5.1 XPU 3.4, 5.5.2 XPU 3.4, 6.0 XPU 3.4, 6.5	RealSecure DHCP Remote Denial of Service	Low	CyberNotes-2002-09
Internet Security Systems ⁷⁰⁸	Windows 95/98/ME/NT 4.0/2000, XP	BlackIce Agent 3.1 EAL	BlackIce Firewall Bypass	Medium	CyberNotes-2002-12
Internet Security Systems ⁷⁰⁹	Multiple	Internet Scanner 6.2.1	Internet Scanner HTTP Banner Buffer Overflow	High	CyberNotes-2002-19
Internet Software Consortium ⁷¹⁰	Unix	INN 2.0-2.2.3	InterNetNews Multiple Vulnerabilities	Medium/High <i>(High if arbitrary code can be executed)</i>	CyberNotes-2002-08
Internet Software Consortium ⁷¹¹	Unix	INN 2.0-2.2.3; SCO OpenLinux 3.1.1 Server, 3.1 Server	INN Multiple Insecure Open Call CVE Name: CAN-2002-0526	Medium	CyberNotes-2002-22
Internet Software Consortium ^{712, 713, 714, 715,}	Unix	DHCPD 3.0, 3.0.1 rc1-rc8	DHCPD NSUPDATE Remote Format String	High	CyberNotes-2002-10
Internet Software Consortium ^{716, 717, 718, 719, 720,}	Unix	BIND 9.0, 9.1-9.1.3, 9.2	ISC BIND 9 Remote Denial Of Service CVE Name: CAN-2002-0400	Low/High	CyberNotes-2002-12
Internet Software Consortium ^{721, 722, 723, 724, 725, 726, 727}	Unix	FreeBSD FreeBSD 4.4-4.7; ISC BIND 8.1-8.1.2, 8.2-8.2.6, 8.3.0-8.3.3; OpenBSD OpenBSD 3.0-3.2	BIND Multiple Vulnerabilities CVE Names: CAN-2002-1219, CAN-2002-1220, CAN-2002-1221	Low/High <i>(High if arbitrary code can be executed)</i>	CyberNotes-2002-23
Invision Power Services ⁷²⁸	Multiple	Invision Board 1.0, 1.0.1	Invision Board ;phpinfo.php' Script	Medium	CyberNotes-2002-20
Iomega ⁷²⁹	Unix	NAS A300U	NAS A300U Multiple Vulnerabilities	Medium	CyberNotes-2002-23

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
iPlanet & Netscape ⁷³⁰	Windows NT 4.0/2000, Unix	iPlanet E-Commerce Solutions, iPlanet Web Server 4.1, 4.1SP1-9, 6.0, 6.0SP1&2; Enterprise Edition 4.1, 4.1SP1-9, 6.0, 6.0SP1&2; Netscape Enterprise Server 3.6	iPlanet Web Server Search Component	High	CyberNotes-2002-14
IPSwitch, Inc. ⁷³¹	Windows NT 4.0/2000	IMail 6.1-6.4, 7.0.1-7.0.4	IMail Domain Administration Privilege Escalation	High	CyberNotes-2002-01
IPSwitch, Inc. ⁷³²	Windows NT 4.0/2000, XP	IMail 5.0, 5.0.5-5.0.8, 6.0-6.0.6, 6.1-6.4, 7.0.1-7.0.7, 7.1	IMail Server LDAP Buffer Overflow	High	CyberNotes-2002-11
IPSwitch, Inc. ⁷³³	Windows NT 3.5.1/4.0/ 2000, XP	IMail 6.0, 6.0.1-6.0.6, 6.1-6.4, 7.0.1-7.0.7	IMail Web Calendaring Denial of Service	Low	CyberNotes-2002-16
IPSwitch, Inc. ⁷³⁴	Windows NT 4.0/2000, XP	WS FTP Server 3.1.1	IPSwitch CPWD Remote Buffer Overflow CVE Name: CAN-2002-0826	High	CyberNotes-2002-16
IPSwitch, Inc. ⁷³⁵	Windows	WS FTP Server 3.1.3	WS FTP Server FTP Bounce and PASV Connection Hijacking	Medium	CyberNotes-2002-22
IRSSI ⁷³⁶	Unix	IRSSI 0.8.4	IRSSI Trojaned Configure File Arbitrary Access	High	CyberNotes-2002-11
Irssi ⁷³⁷	Unix	Irssi 0.8.4	IRSSI Remote Denial of Service	Low	CyberNotes-2002-13
isdn4linux ⁷³⁸	Unix	isdn4linux 3.1 pre1	ISDN4Linux IPPPD Utility Format String	High	CyberNotes-2002-17
Jacob Navia ⁷³⁹	Windows 95/98/ME	lcc-Win32 3.2	LCC-Win32 Compiled Binary Memory Disclosure	Medium	CyberNotes-2002-16
Jacques Gelinat ⁷⁴⁰	Unix	Linuxconf 1.1.6r10, 1.1.7, 1.1.8, 1.1.9r2, 1.1.9r1, 1.2r2, 1.2r1, 1.2, 1.2.1r1-r8, 1.2.1, 1.2.2, 1.2.3r1&2, 1.2.3, 1.2.4r2, 1.2.4r4, 1.2.4r5, 1.2.4, 1.2.7r5, 1.2.7r4, 1.2.7r3, 1.2.7, 1.28r1-r3, 1.28	Linuxconf Local Buffer Overflow	High	CyberNotes-2002-18
Jacques Gelinat ⁷⁴¹	Unix	Linuxconf 1.2.4 r2, 1.2.5 r3	Linuxconf mailconf Module Mail Relay	Medium	CyberNotes-2002-23
Jason Orcutt ⁷⁴²	Windows, Unix	Prometheus 3.0 -beta, 4.0 -beta, 6.0	Prometheus Framework Code Injection CVE Name: CAN-2002-1211	High	CyberNotes-2002-23
Jelsoft Enterprises ⁷⁴³	Multiple	VBulletin 2.2.0	VBulletin Board Cross-Site Scripting	High	CyberNotes-2002-03
Jelsoft Enterprises ⁷⁴⁴	Windows, Unix	VBulletin	VBulletin Calendar.PHP Command Execution	High	CyberNotes-2002-20
Jelsoft Enterprises ⁷⁴⁵	Windows, Unix	VBulletin 2.0 rc3, rc2, 2.2.0- 2.2.8	VBulletin Cross-Site Scripting	High	CyberNotes-2002-22
Jelsoft Enterprises ⁷⁴⁶	Unix	VBulletin 2.0 rc 2&3, 2.0.3, 2.2.0-2.2.9	VBulletin Cross-Site Scripting	High	CyberNotes-2002-24
Jelsoft Enterprises ⁷⁴⁷	Unix	VBulletin 2.0-2.0.2, 2.2.0- 2.2.9 can	VBulletin members2.php Cross Site Scripting	High	CyberNotes-2002-24
Jerrett Taylor ⁷⁴⁸	Multiple	PHP ImgList 1.1, 1.2, 1.2.1	PHP ImgList Directory Traversal	Medium	CyberNotes-2002-06
Jetty ⁷⁴⁹	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	Jetty 3.1.6, 3.1.7, 4.1.0RC4	Jetty CGIServlet Arbitrary Command Execution	High	CyberNotes-2002-20
Jetty ⁷⁵⁰	Unix	Jetty 4.1	Jetty HTTP Cross-Site Scripting	High	CyberNotes-2002-20
Jetty ⁷⁵¹	Unix	Jetty 4.1 .0RC4	Jetty Cross-Site Scripting	High	CyberNotes-2002-20
jmece ⁷⁵²	Unix	jmece 1.3.8	jmece Symbolic Link	High	CyberNotes-2002-02
Joe DePasquale ⁷⁵³	Multiple	Bannermatic 1.0, 2.0, 3.0	Bannermatic World Readable Data Files	Medium	CyberNotes-2002-10
Joe Testa ⁷⁵⁴	Multiple	hellbent 0.1	hellbent Relative Path Information Disclosure and 'hellbent.prefs' GET Request	Medium	CyberNotes-2002-02
John G. Myers ⁷⁵⁵	Unix	Mpack 1.5	Mpack Buffer Overflow & Malformed Filename	Low/ High (High if arbitrary code is executed)	CyberNotes-2002-16

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
John Hardin ⁷⁵⁶	Multiple	Procmil Email Sanitizer 1.131, 1.132	Procmil Email Sanitizer Multipart Mime Recognition	Medium	CyberNotes-2002-01
John Roy ⁷⁵⁷	Windows 95/98/NT 4.0/2000	Pi3Web for Windows 2.0	Pi3Web For Windows buffer Overflow	High	CyberNotes-2002-02
John Roy ⁷⁵⁸	Windows 95/98/NT 4.0/2000	Pi3Web 1.0.1, 1.0.3, Pi3Web for Windows 2.0.0	Pi3Web Path Disclosure	Medium	CyberNotes-2002-06
Jon Hedley ⁷⁵⁹	Multiple	AlienForm2 1.5	AlienForm2 Directory Traversal	Medium	CyberNotes-2002-12
Jon Howell ⁷⁶⁰	Multiple	Faq-O-Matic 2.711, 2.712	Faq-O-Matic Cross-Site Scripting	High	CyberNotes-2002-09
Joseph Allen ⁷⁶¹	Unix	joe 2.8, 2.9, 2.9.1, 2.9.2, 2.9.4-2.9.7	Joe Text Editor Backup SetUID Executable Editing Permission Elevation	High	CyberNotes-2002-19
Julian Field ⁷⁶²	Unix	Mail Scanner 3.2 5-1, 3.2 4-1, 3.2 3-1 -3.2.3-5, 4.0 4-1, 4.0 3-1, 4.0 2-3, 4.0 2-2, 4.0 2-1	MailScanner Attachment Filename Bypass	Medium	CyberNotes-2002-23
KDE ⁷⁶³	Unix	KDEUtils 2.2-2, 2.2	KDE2 KDEUtils KLPRFax_Filter Insecure Temporary File Creation	High	CyberNotes-2002-01
KDE ⁷⁶⁴	Unix	KDE 2.1-2.2.2, 3.0, 3.0.2	KDE Konqueror Oversized Image Width Denial of Service	Low	CyberNotes-2002-19
KDE ⁷⁶⁵	Unix	KDE 3.0-3.0.2	KDE Secure Cookie Exposure	Medium	CyberNotes-2002-19
KDE ⁷⁶⁶	Unix	KDE 3.0.1-3.0.3	KDE KPF Directory Traversal	Medium	CyberNotes-2002-21
KDE ⁷⁶⁷ <i>More vendors release patches</i> ^{768, 769, 770}	Unix	KDE 2.1-2.2.2, 3.0-3.0.4	KDE KIO Subsystem Network Protocol Implementation	High	CyberNotes-2002-24 CyberNotes-2002-25
KDE ^{771, 772}	Unix	KDE 2.2.2, 3.0, 3.0.1-3.0.3, Konqueror 2.2.2, 3.0, 3.0.1-3.0.3	KDE Konqueror Sub-Frames Script Execution	High	CyberNotes-2002-19
KDE ^{773, 774, 775, 776}	Unix	KDE 2.0-2.2, 3.0-3.0.4, klisa 2.2.2; LISa LISa 0.1, 0.1.2	KDE Network Buffer Overflow CVE Name: CAN-2002-1247	High	CyberNotes-2002-23
Kerio ⁷⁷⁷	Windows NT	MailServer 5.0, 5.1, 5.1.1	MailServer Multiple Denial of Service & Cross-Site Scripting Vulnerabilities	Low/High (High if arbitrary code is executed)	CyberNotes-2002-17
Kerio ⁷⁷⁸	Windows NT 4.0/2000	Personal Firewall 2 2.1-2.1.4	Personal Firewall Denial of Service	Low/High (High if DoS best practices not in place)	CyberNotes-2002-18
Key Focus ⁷⁷⁹	Windows 95/98/ME/NT 4.0/2000, XP	KF Web Server 1.0.2	KF Web Server Directory Contents Disclosure	Medium	CyberNotes-2002-14
KeyFocus Ltd. ⁷⁸⁰	Windows 98/ME/ 2000, XP	KF Web Server 1.0.8	KF Web Server Directory Traversal	Medium	CyberNotes-2002-24
KGPG ⁷⁸¹	Unix	KGPG 0.6-0.8.2	KGPG Key Generation	Medium	CyberNotes-2002-23
Khaled MardamBey ⁷⁸²	Windows 95/98/ME/NT 4.0/2000, XP	mIRC 2.1a, 2.3a, 2.4, 2.4a, 2.5a, 2.7a, 2.8c, 3.1-3.9, 4.0, 4.1, 4.5-4.7, 5.0, 5.1, 5.3-5.91	mIRC Nickname Buffer Overflow	High	CyberNotes-2002-03
Khaled MardamBey ⁷⁸³	Windows 95/98/ME/NT 4.0/2000, XP	mIRC 6.0, 6.01	mIRC DCC Sensitive Information	Medium	CyberNotes-2002-05
Khaled MardamBey ⁷⁸⁴	Windows 95/98/ME/ NT 4.0/2000, XP	mIRC 6.0-6.0.2	mIRC ASCTime Buffer Overflow	High	CyberNotes-2002-18
KICQ ⁷⁸⁵	Unix	KICQ 2.0.0b1	KICQ Denial of Service	Low	CyberNotes-2002-03
Killer Protection ⁷⁸⁶	Multiple	Killer Protection 1.0	Killer Protection Information Disclosure	Medium	CyberNotes-2002-21
KillerVault ⁷⁸⁷	Multiple	Kv Guestbook 1.0	Kv Guestbook Cross-Site Scripting	High	CyberNotes-2002-09
KillerVault ⁷⁸⁸	Multiple	kv Poll 1.1	kv Poll Corrupt Poll Data	Medium	CyberNotes-2002-10

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Kim Storm ⁷⁸⁹	Unix	NN 6.6.0- 6.6.3	NN Format String	High	CyberNotes-2002-14
KisMAC ⁷⁹⁰	Unix	KisMAC 0.02a, 0.01c, 0.01b, 0.01a	KisMAC Insecure File Permissions	Medium	CyberNotes-2002-25
Kismet Project ⁷⁹¹	Unix	Kismet 2.2, 2.2.1	Kismet Remote Command Execution	High	CyberNotes-2002-11
KMail ⁷⁹²	Unix	KDE KMail 1.2	KMail Denial Of Service	Low	CyberNotes-2002-05
kmMail ⁷⁹³	Unix	kmMail 1.0 b & prior	kmMail E-Mail Cross-Site Scripting	High	CyberNotes-2002-22
KTH ⁷⁹⁴	Unix	Kerberos 4 1.0.2-1.0.4, 1.1.1	Kerberos4 FTP Bounds Checking	High	CyberNotes-2002-09
KTH ⁷⁹⁵ <i>SuSE releases patches⁷⁹⁶</i>	Unix	Heimdal 0.4 a-0.4 e	Kerberos Forwarding Daemon File Overwriting	Medium/High (High if root is exploited)	CyberNotes-2002-19 CyberNotes-2002-20
Kunani ⁷⁹⁷	Windows	Kunani FTP Server 1.0.10	Kunani FTP Server Directory Traversal	Medium	CyberNotes-2002-25
l2tpd ⁷⁹⁸	Unix	l2tpd 0.62-0.67	L2TPD Weak Random Number Generator	Medium	CyberNotes-2002-17
Larry Wall ⁷⁹⁹	Unix	Perl 5.6	SuidPerl Information Disclosure	Medium	CyberNotes-2002-25
Lawson Software ⁸⁰⁰	Unix	Lawson Financials 8.0	Lawson Financials Account Credentials World Accessible	Medium	CyberNotes-2002-25
LBL ⁸⁰¹	Unix	libpcap 0.7.1, tcpdump 3.6.2, 3.7.1	TCPDump / LIBPCap Trojan Horse	Medium	CyberNotes-2002-23
LBL ⁸⁰²	Unix	tcpdump 3.4 a6, 3.4, 3.5, 3.5.2, 3.6.2	TCPDump Memory Corruption	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-24
LBL ^{803, 804, 805, 806, 807, 808}	Unix	tcpdump 3.6.2	TCPDump Malformed NFS Packet Buffer Overflow CVE Name: CAN-2002-0380	High	CyberNotes-2002-12
Lebios ⁸⁰⁹	Multiple	PHPToNuke. php 1.0	PHPNuke AddOn PHPToNuke. PHP Cross-Site Scripting	High	CyberNotes-2002-01
Legato ⁸¹⁰	Windows NT 4.0/2000, Unix	NetWorker 6.1	NetWorker Plaintext	Medium	CyberNotes-2002-02
Les VanBrunt ⁸¹¹	Unix	AdRotate Pro 2.0	AdRotate Pro SQL Injection	High	CyberNotes-2002-01
Leszek Krupinski ⁸¹²	Multiple	L-Forum 2.4 .0	L-Forum Multiple Vulnerabilities	Medium/High (High if arbitrary code is executed)	CyberNotes-2002-17
Leung Eric ⁸¹³	Unix	E-Guest 1.1	E-Guest Book Script Injection	High	CyberNotes-2002-14
LEVCGI.COM ⁸¹⁴	Multiple	NetPad 1.0-1.0.2	NetPad Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-10
LEVCGI.COM ⁸¹⁵	Unix	MyGuestbook 1.0	MyGuestbook Script Injection	High	CyberNotes-2002-09
LG Electronics ⁸¹⁶	Multiple	LR3001f 4.0, LR3100p 1.50, LR3100p 1.30	LR Series WAN Router Denial of Service	Low	CyberNotes-2002-17
LG Electronics ⁸¹⁷	Multiple	LR3001f 4.0, LR3001f 4.57, LR3100p 1.50, LR3100p 1.30	LR Series Telnet Daemon Buffer Overflow	Low	CyberNotes-2002-17
Lib CGI ⁸¹⁸	Unix	Lib CGI 0.1	Lib CGI Include Buffer Overflow	Medium	CyberNotes-2002-24
LibPNG ⁸¹⁹ <i>SCO issues patch⁸²⁰</i>	Unix	LibPNG 1.0.12	LibPNG Wide Image Processing CVE Name: CAN-2002-0728	High	CyberNotes-2002-16 CyberNotes-2002-23
LICQ ⁸²¹	Unix	LICQ 1.0-1.0.4	LICQ Format String Denial Of Service	Low	CyberNotes-2002-03
LIDS ⁸²²	Unix	LIDS 1.1 & prior	LIDS Capability Leakage via LD PRELOAD	High	CyberNotes-2002-01
Light httpd ⁸²³	Windows, Unix	Light HTTPD 0.1	Light HTTPD Buffer Overflow	High	CyberNotes-2002-23

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Linksys Group Inc. ⁸²⁴	Unix	EtherFast BEFN2PS4 Router, BEFSR81 Router	Linksys DSL Router SNMP Trap System Arbitrary Sending and Default SNMP Community String Vulnerabilities	Low/ Medium	CyberNotes-2002-01
Linksys Group Inc. ⁸²⁵	Multiple	EtherFast BEFVP41 Router 0.0	EtherFast BEFVP41 Key Weak Encryption	Medium	CyberNotes-2002-06
Linksys Group Inc. ⁸²⁶	Multiple	EtherFast BEFSR11 Router 1.42.7, BEFSR41 Router 1.42.7, BEFSRU31 Router 1.42.7	EtherFast Router Remote Administration Enabled	High	CyberNotes-2002-12
Linksys Group Inc. ⁸²⁷	Multiple	WET11 Wireless Ethernet Bridge	WET11 Remote Denial of Service	Low	CyberNotes-2002-22
Linksys Group Inc. ⁸²⁸	Multiple	BEFN2PS4 1.42.7, BEFSX41 1.42.7, BEFVP41 1.42.7, BEFW11S4 1.4.2.7, 1.4.3, EtherFast BEFSR11 Router 1.42.7, 1.43, BEFSR41 Router 1.42.7, 1.43, BEFSR81 Router 2.42.7, BEFSRU31 Router 1.42.7, 1.43, HPRO200 1.42.7	Multiple Linksys Devices Password Field Buffer Overflow CVE Name: CAN-2002-1312	Low	CyberNotes-2002-24
Linksys Group Inc. ⁸²⁹	Multiple	BEFN2PS4 1.42.7, BEFSX41 1.43, 1.43.3, 1.43.4, BEFW114 1.4.2.7, 1.4.3, 1.43.3, EtherFast BEFSR11 Router 1.42.7, 1.43, 1.43.3, EtherFast BEFSR41 Router 1.42.7, 1.43, 1.43.3, EtherFast BEFSR81 Router, EtherFast BEFSR81 Router 2.42.7, BEFSRU31 Router 1.42.7, 1.43, 1.43.3	Multiple Linksys Vulnerabilities	Medium High (High if arbitrary code can be executed)	CyberNotes-2002-25
Linksys Group, Inc. ⁸³⁰	Multiple	EtherFast BEFSR41 Router 1.40.2, 1.41, 1.42.3, 1.42.7	Linksys BEFSR41 Denial of Service CVE Name: CAN-2002-1236	Low	CyberNotes-2002-23
Linksys Group, Inc. ⁸³¹	Multiple	BEFW11S4 1.4.2.7, 4 1.4.3; EtherFast BEFSR11 Router 1.41, 1.42.3, 1.42.7, 1.43; BEFSR41 Router 1.41, 1.42.3, 1.42.7, 1.43; BEFSRU31 Router 1.41, 1.42.3, 1.42.7, 1.43	Linksys Router Unauthorized Management Access	High	CyberNotes-2002-24
Linux Directory ⁸³²	Unix	Penguin Traceroute 1.0	Penguin Traceroute Arbitrary Command Execution	High	CyberNotes-2002-06
Linux Kernel ⁸³³	Unix	kernel 2.4.18 pre-1-8, 2.4.18, 2.4.19 -pre1-6	Linux Kernel Multiple Security Issues	Medium	CyberNotes-2002-17
Linux-Sottises ⁸³⁴	Unix	Board-TNK 1.3, News-TNK 1.2.1	Board-TNK & News-TNK Cross Site Scripting	High	CyberNotes-2002-06
Livre Dor ⁸³⁵	Multiple	Livre Dor' 1.1	Livre Dor' Information Disclosure	Medium	CyberNotes-2002-09
LocalWEB2000 ⁸³⁶	Windows 98/NT 4.0/2000	LocalWEB 2000 2.1.0 Standard Version	LocalWEB File Disclosure	Medium	CyberNotes-2002-11
LogiSense Corporation ⁸³⁷	Multiple	DNS Manager System, Hawk-i 5.2, Hawk-i ASP	Hawk-i ASP Login	Medium	CyberNotes-2002-12
Logitech ⁸³⁸	Windows NT 4.0/2000, XP	Cordless Freedom iTouch Keyboard, Cordless iTouch Keyboard	iTouch Keyboard Command Keys Locked Console Bypass	Low	CyberNotes-2002-09
Logsurfer ⁸³⁹	Windows, Unix	Logsurfer 1.5 a, 1.5, 1.41	Logsurfer Buffer Overflows	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-21
LogWatch ⁸⁴⁰ <i>RedHat issues update⁸⁴¹</i>	Unix	LogWatch 2.1.1	LogWatch Root Compromise	High	CyberNotes-2002-07 CyberNotes-2002-08
Lokwa ⁸⁴²	Multiple	Lokwa BB 1.2.1	Lokwa BB Sensitive Information	Medium	CyberNotes-2002-12
Lonerunner ⁸⁴³	Windows, Unix	Zeroo HTTP Server 1.5	Zeroo HTTP Server Remote Buffer Overflow	High	CyberNotes-2002-24

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Lotus ⁸⁴⁴	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Domino 4.6.1, 4.6.3, 4.6.4, 5.0, 5.0.1-5.0.9	Domino DOS Request Denial Of Service	Low	CyberNotes-2002-03
Lotus ⁸⁴⁵	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Domino 5.0. 5.0.1-5.0.9	Domino Remote Authentication Bypass	Medium	CyberNotes-2002-03
Lotus ⁸⁴⁶	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Domino 5.0- 5.0.8	Domino Information Disclosure	Medium	CyberNotes-2002-04
Lotus ⁸⁴⁷	Unix	Domino R4 (version 4.x)	Domino File Retrieval	Medium	CyberNotes-2002-14
Lotus ⁸⁴⁸	Multiple	Lotus Domino 5.0.8, 5.0.9a, 5.0.9	Lotus Domino NSF Database Banner Information Disclosure	Medium	CyberNotes-2002-23
Luca Deri ⁸⁴⁹	Unix	ntop 2.0	ntop Remote Format String	High	CyberNotes-2002-05
Lucent Technologies ⁸⁵⁰	Multiple	Access Point 1500 Service Router, 300 Service Router , 600 Service Router	Lucent Access Point IP Services Router Long HTTP Request Denial Of Service	Low	CyberNotes-2002-16
Lucent Technologies ⁸⁵¹	Multiple	Ascend MAX 5.0 .0Ap42, Pipeline 5.0.0A, MAX Router 1.0-5.0, 5.0 ap48, Pipeline Router 1.0-6.0, 6.0.2, DSL Terminator	Multiple Lucent Router UDP Port 9 Information Disclosure	Medium	CyberNotes-2002-16
Lucent Technologies ⁸⁵²	Multiple	VPN Firewall Brick 1000, 20, 201, 80	Lucent Brick Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained)	CyberNotes-2002-16
Ludovic STIOT ⁸⁵³	Multiple	Secure 17/09/2001	Secure Authentication Bypass	Medium	CyberNotes-2002-09
Luis Bernardo ⁸⁵⁴	Multiple	MyHelp Desk 20020509	MyHelpDesk Multiple Vulnerabilities	High	CyberNotes-2002-12
Lumigent ⁸⁵⁵	Windows	Log Explorer 3.0 1	Log Explorer XP_LogAttach_StartProf, XP_LogAttach_SetPort & XP_LogAttachBuffer Overflows	High	CyberNotes-2002-13
Lycos ⁸⁵⁶	Multiple	htmlGEAR guest GEAR	guestGear CSS HTML Injection	High	CyberNotes-2002-19
LYSIAS Organization ⁸⁵⁷	Windows	Lidik Webserver 0.7 b	Lidik Webserver Directory Traversal	Medium	CyberNotes-2002-10
Macromedia Inc. ⁸⁵⁸	Windows 95/98/ME/NT 4.0/2000, XP	Macromedia Flash 5.0	Macromedia Flash Undocumented Command & Undocument File Access	High	CyberNotes-2002-06
Macromedia Inc. ⁸⁵⁹	Multiple	Flash 6.0	Flash ActiveX Buffer Overflow	High	CyberNotes-2002-09
Macromedia Inc. ⁸⁶⁰	Multiple	Dream weaver 4.0, Ultradev 4.0	Dreamweaver InterDev SQL Injection	Medium	CyberNotes-2002-10
Macromedia Inc. ⁸⁶¹	Multiple	JRun 3.0, 3.1, 4.0	JRun JSP Page Denial of Service	Low	CyberNotes-2002-12
Macromedia Inc. ⁸⁶²	Windows	ColdFusion Server MX Professional, Enterprise, Developer	ColdFusion MX jrun.dll Denial of Service	Low	CyberNotes-2002-14
Macromedia Inc. ⁸⁶³	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	JRun Authentication Bypass	Medium	CyberNotes-2002-14
Macromedia Inc. ⁸⁶⁴	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	Macromedia JRun Source Disclosure	Medium	CyberNotes-2002-14
Macromedia Inc. ⁸⁶⁵	Multiple	Sitespring 1.2.0	Sitespring Denial of Service	Low	CyberNotes-2002-14
Macromedia Inc. ⁸⁶⁶	Windows	Sitespring 1.2 .0	Sitespring Cross-Site Scripting	High	CyberNotes-2002-15

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Macromedia Inc. ⁸⁶⁷ <i>Vulnerability appears in Press</i> ⁸⁶⁸	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Flash 5.0, 6.0, 6.0.29.0	Flash Malformed Header Buffer Overflow	High	CyberNotes-2002-16 CyberNotes-2002-17
Macromedia Inc. ⁸⁶⁹	Multiple	Flash 6.0, 6.0.29.0, 6.0.40.0	Flash Player Arbitrary Local File Access	Medium	CyberNotes-2002-16
Macromedia Inc. ⁸⁷⁰	Windows 95/98/ME/ NT 4.0/2000, XP	Flash 4.0 r12, 5.0 r50, 5.0, 6.0, 6.0.29.0, 6.0.40.0, 6.0.47.0	Flash Malformed SWF Denial of Service	Low	CyberNotes-2002-17
Macromedia Inc. ⁸⁷¹	Multiple	Flash 6.0, 6.0.29.0, 6.0.40.0, 6.0.47.0	Flash Player Remote SMB Shares File Access	Medium	CyberNotes-2002-21
Macromedia Inc. ⁸⁷²	Windows NT	Flash 6.0.47.0	Flash SWRemote Heap Corruption	High	CyberNotes-2002-24
Macromedia Inc. ⁸⁷³	Multiple	ColdFusion Server MX 6.0, JRun 4.0, 4.0SP1a, 4.0 SP1	JRun 4/ ColdFusion XML Parser Denial of Service	Low	CyberNotes-2002-25
Macromedia, Inc. ⁸⁷⁴	Windows NT 4.0/2000, Unix	JRun 3.0, 3.1	JRun Header Field Buffer Overflow	High	CyberNotes-2002-11
Macromedia, Inc. ⁸⁷⁵	Windows NT 4.0/2000, Unix	ColdFusion Server MX Professional, MX Enterprise, MX Developer	ColdFusion MX CFML Source Disclosure	Medium	CyberNotes-2002-23
Macromedia, Inc. ⁸⁷⁶	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	JRun IIS ISAPI Remote Buffer Overflow	High	CyberNotes-2002-23
Macromedia, Inc. ⁸⁷⁷	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	JRun Log File/JRun.INI File Disclosure	Medium	CyberNotes-2002-23
Macromedia, Inc. ⁸⁷⁸	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	JRun Web Server Unicode Source Disclosure	Medium	CyberNotes-2002-23
MailEnable ⁸⁷⁹	Windows NT	MailEnable 1.5 015- 1.5 018	MailEnable E-mail Server Buffer Overflow	High	CyberNotes-2002-24
Mailreader.com ⁸⁸⁰	Unix	Mailreader.com 2.3.20- 2.3.31	MailReader.com Directory Traversal & Remote Command Execution	Medium/High (High if arbitrary can be executed)	CyberNotes-2002-22
Mandrake Soft ⁸⁸¹	Unix	Linux Mandrake 8.0, 8.0 ppc, 8.1 ia64, 8.1	Mandrake Bind 9 Package Insecure File Permissions	Medium	CyberNotes-2002-01
Mandrake Soft ⁸⁸²	Unix	Linux Mandrake 8.2	Mandrake 8.2 Msec Insecure Default Permissions	Medium	CyberNotes-2002-13
Mantis ⁸⁸³	Unix	Mantis 0.15.3- 0.15.12, 0.16.0, 0.16.1, 0.17.0- 0.17.2	Mantis Account Update	Medium	CyberNotes-2002-17
Mantis ⁸⁸⁴	Unix	Mantis 0.15.3- 0.15.12, 0.16.0, 0.16.1, 0.17.0- 0.17.3	Mantis JPGraph Remote Command Execution	High	CyberNotes-2002-17
Mantis ⁸⁸⁵	Unix	Mantis 0.15.3- 0.15.12, 0.16.0, 0.16.1, 0.17.0- 0.17.3	Mantis Unauthorized Project Viewing	Medium	CyberNotes-2002-17
Mantis ⁸⁸⁶	Unix	Mantis 0.16.0, 0.17.0- 0.17.3	Mantis Limit Reporters Option Bypass	Medium	CyberNotes-2002-17
Mantis ⁸⁸⁷	Unix	Mantis 0.17.0- 0.17.3	Mantis Remote File Include Command Execution	High	CyberNotes-2002-17
Mantis ⁸⁸⁸	Unix	Mantis 0.17.0- 0.17.4, 0.17.4a	Mantis Unauthorized Bug Viewing	Medium	CyberNotes-2002-18
Mantis ⁸⁸⁹	Unix	Mantis 0.17.0- 0.17.4, 0.17.4a	Mantis Unauthorized Project Bug List Viewing	Medium	CyberNotes-2002-18
Marc Druilhe ⁸⁹⁰	Multiple	W-Agora 4.1.1-4.1.3	W-Agora Arbitrary Code Execution	High	CyberNotes-2002-12
Marcus S. Xenakis ⁸⁹¹	Unix	Unix Manual 1.0	manual.php Arbitrary Shell Command Execution	High	CyberNotes-2002-01

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Marcus S. Xenakis ⁸⁹²	Unix	Directory. php 0.0	Directory.php Arbitrary Code Execution	High	CyberNotes-2002-06
Mark Hanson ⁸⁹³	Windows	XiRCON 1.0 Beta 4	XiRCON Remote Denial of Service	Low	CyberNotes-2002-14
Mark Ruef ⁸⁹⁴	Unix	Virgil CGI Scanner 0.9	Virgil CGI Scanner Remote Command Execution	High	CyberNotes-2002-22
Markus Kliegl ⁸⁹⁵	Unix	mod bf 0.2	mod bf Buffer Overflow	High	CyberNotes-2002-01
Martin Bauer ⁸⁹⁶	Windows, Unix	gBook 1.4	gBook Administrative Access	High	CyberNotes-2002-22
Martin Roesch ⁸⁹⁷	Unix	Snort 1.8.3	Snort ICMP Denial of Service	Low	CyberNotes-2002-02
MasqMail ⁸⁹⁸	Unix	MasqMail 0.1.16	MasqMail Buffer Overflow	High	CyberNotes-2002-23
Matsushita Research ⁸⁹⁹	Unix	MNews 1.2.2	MNews Multiple Buffer Overflows	Medium	CyberNotes-2002-12
Matt Blaze ⁹⁰⁰	Unix	cfs 1.3.3 Sparc, PPC, m68k, ia32, ARM, Alpha	CFS Multiple Buffer Overflows	Low	CyberNotes-2002-05
Matt Wright ⁹⁰¹	Unix	FormMail 1.0-1.9	FormMail SCI Script Vulnerabilities	High	CyberNotes-2002-02
Matthew Mondor ⁹⁰²	Unix	mmftpd .7	MMFTPD SysLog Format String	High	CyberNotes-2002-12
Matthew Mondor ⁹⁰³	Unix	MMMail .11, .12, .13	MMMail Remote SysLog Format String	High	CyberNotes-2002-12
Matu ⁹⁰⁴	Multiple	Matu FTP 1.74	Matu FTP Client Buffer Overflow	High	CyberNotes-2002-09
Matu ⁹⁰⁵	Windows 95/98	Matu FTP 1.13	Matu FTP Server Buffer Overflow	High	CyberNotes-2002-11
McMurtrey/Whitaker & Associates ⁹⁰⁶	Windows 98/ME/NT 4.0/2000	Cart32 2.5a, 2.6, 3.0, 3.1, 3.5a Build 710, 3.5a, 3.5 Build 619, 3.5, 4.4	Cart32 Insufficient Validation Hidden Form Field	Medium	CyberNotes-2002-24
McNews ⁹⁰⁷	Multiple	McNews 1.0-1.2	McNews File Disclosure	Medium/High (High is arbitrary code can be executed)	CyberNotes-2002-11
MDG Computer Services, Inc. ⁹⁰⁸	Windows 98/NT 4.0, MacOS X 10.0	Web Server 4D/ eCommerce 3.5.3	Web Server 4D/ eCommerce Directory Traversal	Medium	CyberNotes-2002-02
MDG Computer Services, Inc. ⁹⁰⁹	Windows 98/NT 4.0, MacOS X 10.0	Web Server 4D/ eCommerce 3.5.3	Web Server 4D/ eCommerce Denial of Service	Low	CyberNotes-2002-02
MDG Computer Services, Inc. ⁹¹⁰	Windows NT 4.0/2000, MacOS	Web Server 4D 3.6	MDG Web Server 4D Insecure Credential Storage	Medium	CyberNotes-2002-20
Melange ⁹¹¹	Multiple	Melange Chat System 2.0.2 Beta 2	Melange Chat Systems Multiple Buffer Overflows	Medium	CyberNotes-2002-08
MenaSoft ⁹¹²	Windows 95/98/NT 4.0/2000, Unix	SPHER Eserver 0.99l, 0.99f	SPHEREserver Denial of Service	Low	CyberNotes-2002-06
Messagerie ⁹¹³	Multiple	Messagerie 1.0	Messagerie Denial of Service	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-09
MetaLinks ⁹¹⁴	Multiple	MetaCart2.sql	MetaCart2. SQL Database Disclosure	Medium	CyberNotes-2002-13
Meteor Soft ⁹¹⁵	Windows 98/ME	Meteor FTP 1.2b	Meteor FTP Multiple Denial of Service Vulnerabilities	Low	CyberNotes-2002-11
Mewsoft ⁹¹⁶	Multiple	NetAuction 3.0	NetAuction Cross-Site Scripting	High	CyberNotes-2002-13
MHOnArc ⁹¹⁷	Multiple	MHOnArc 2.5, 2.5.1, 2.5.2	MHOnArc HTML Script Filter Bypass	High	CyberNotes-2002-08

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
MHonArc ⁹¹⁸	Unix	MHonArc 2.4.4, 2.5.2, 2.5.13	MHonArc Mail Cross-Site Scripting CVE Name: CAN-2002-1307	High	CyberNotes-2002-24
Michael Behan ⁹¹⁹	Multiple	CodeBlue 5.1	CodeBlue SMTP Response Buffer Overflow	High	CyberNotes-2002-15
Michael Krax ⁹²⁰	Unix	log2mail 0.2.5 .0	log2mail Remote Buffer Overflow	High	CyberNotes-2002-23
Michael Lamont ⁹²¹	Windows 95/98/NT 4.0/2000	Savant WebServer 3.0	Savant Web Server Long Request Denial of Service	Low	CyberNotes-2002-01
Michael Schatz ⁹²²	Multiple	Books 0.6, 0.54	Books PostNuke Module Cross-Site Scripting	High	CyberNotes-2002-20
Microsoft ⁹²³	Windows 95/98/ME/NT 4.0/2000	Excel 97, 97SR2&2, 2000, 2002	Excel Spreadsheet Data Password Protection Bypass	Medium	CyberNotes-2002-01
Microsoft ⁹²⁴	Unix	Internet Explorer 5.0 SP1 Solaris	Internet Explorer for Solaris X Server Denial of Service	Low	CyberNotes-2002-01
Microsoft ⁹²⁵	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.01, Internet Explorer 5.01SP1&2, 5.5, .5SP1&2	Internet Explorer JavaScript Local File Enumeration	Medium	CyberNotes-2002-01
Microsoft ⁹²⁶	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2, 6.0	Internet Explorer Same Origin Policy Violation	High	CyberNotes-2002-01
Microsoft ⁹²⁷	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2, 6.0	Internet Explorer Refresh Denial of Service	Low	CyberNotes-2002-01
Microsoft ⁹²⁸	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2, 6.0	Internet Explorer GetObject File Disclosure	High	CyberNotes-2002-01
Microsoft ⁹²⁹	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2, 6.0	Internet Explorer Modeless Dialog Denial of Service	Low	CyberNotes-2002-01
Microsoft ⁹³⁰	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	Internet Explorer XMLHTTP File Disclosure	Medium	CyberNotes-2002-01
Microsoft ⁹³¹	Windows NT 4.0/2000, XP	SQL Server 7.0, 2000	SQL Server C Runtime Library Format String and Buffer Overflow CVE Names: CAN-2001-0542, CAN-2001-0879	Low/ High (High for the buffer overflow vulnerabilities.)	CyberNotes-2002-01
Microsoft ⁹³²	Windows 98/98SE/ME/XP	Windows 98, 98SE, ME, XP	Windows UPnP NOTIFY Buffer Overflow and Denial of Service Distributed Denial of Service CVE Names: CAN-2001-0876, CAN-2001-0877	Low/High (High for the buffer overflow UPnP vulnerability.)	CyberNotes-2002-01
Microsoft ⁹³³	Windows XP	Windows XP	Windows XP Unauthorized Hotkey Program	Medium	CyberNotes-2002-01
Microsoft ⁹³⁴	Windows XP	Windows XP	Windows XP Multiple Security Vulnerabilities	Medium	CyberNotes-2002-01
Microsoft ⁹³⁵	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.01, 5.0, 5.5, 6.0	Internet Explorer 'clipboardData'	Medium	CyberNotes-2002-02
Microsoft ⁹³⁶	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2	Internet Explorer Form Denial of Service	Low	CyberNotes-2002-02
Microsoft ⁹³⁷	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	Internet Explorer Arbitrary Execution	High	CyberNotes-2002-02
Microsoft ⁹³⁸	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0, Windows XP Professional	Windows XP Pro Upgrade	Medium	CyberNotes-2002-02

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ⁹³⁹	MacOS 7.0/8.0/9.0	Internet Explorer Macintosh Edition 3.0-4.0.1, 4.5, 5.0	MacOS Internet Explorer File Path	High	CyberNotes-2002-02
Microsoft ⁹⁴⁰	Windows NT 4.0	Windows 4.0, NT 4.0SP1-SP6a, NT Enterprise Server 4.0, 4.0SP1-SP6a, NT Server 4.0, 4.0SP1-SP6a, NT Workstation 4.0, 4.0SP1- SP6a	Windows NT Locked Account	Medium	CyberNotes-2002-02
Microsoft ⁹⁴¹	Windows 95	Windows 95, 95 SR2	Microsoft Backup Buffer Overflow	High	CyberNotes-2002-02
Microsoft ⁹⁴²	Windows XP	Windows XP Home, Windows XP Professional	Windows XP XML Denial of Service	Low	CyberNotes-2002-02
Microsoft ⁹⁴³	Windows 2000	Exchange Server 2000, 2000 SP1&2	Exchange Inappropriate Registry Permissions CVE Name: CAN-2002-0049	Medium	CyberNotes-2002-03
Microsoft ⁹⁴⁴	Windows NT 4.0/2000	IIS 5.0, SQL Server 6.5, 7.0, 7.0 SP1-3, 7.0SP1-3 alpha, 2000, 2000 SP1-2, 2000 Advanced Server, 2000 Advanced Server SP1-2, 2000 Datacenter Server, 2000 Datacenter Server SP1-2, 2000 Professional, 2000 Professional SP1-2, 2000 Server, 2000 Server SP1-2	Microsoft MSDTC Service Denial of Service	Low	CyberNotes-2002-03
Microsoft ⁹⁴⁵	Windows NT 4.0/2000	Interix 2.2; Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 ServerSP1&2, 2000 Terminal Services, 2000 Terminal Services SP1&2	Telnet Server Unchecked Buffer CVE Name: CAN-2002-00020	High	CyberNotes-2002-03
Microsoft ⁹⁴⁶	Windows 95/98/ME/NT 4.0/2000, XP	MSN Messenger Service 4.5, 4.6	MSN ActiveX Sensitive Information Disclosure	Medium	CyberNotes-2002-03
Microsoft ⁹⁴⁷	MacOS X 10.0-10.1.2	Office v. X	Office v. X for Macintosh PID Checker Denial of Service CVE Name: CAN-2002-0021	Low	CyberNotes-2002-03
Microsoft ⁹⁴⁸	Windows NT 4.0	Site Server 3.0 with SP3 & prior, Commerce Edition 3.0 SP4 & prior	Site Server Multiple Vulnerabilities	Low/ Medium/High (Medium if sensitive information can be accessed and High if arbitrary code can be executed)	CyberNotes-2002-03
Microsoft ⁹⁴⁹ <i>Bulletin has been revised⁹⁵⁰</i>	Windows NT 4.0/2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Server, 2000 Server SP1&2, NT Enterprise Server 4.0, NT Enterprise Server 4.0 SP1-6a, NT Server 4.0, NT Server 4.0 SP1-6a	Windows Trusted Domain Membership CVE Name: CAN-2002-0018	Medium	CyberNotes-2002-03 CyberNotes-2002-09
Microsoft ⁹⁵¹	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, 2000 Advanced Server SP2SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2, 2000 Server Japanese Edition, 4.0, 4.0 alpha, 4.0 SP1-5, 4.0 SP1-5 alpha, XP, XP Home, XP Professional	Windows NTFS File Hiding	Medium	CyberNotes-2002-03

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ⁹⁵²	Windows 2000	Commerce Server 2000	Commerce Server 2000 ISAPI Buffer Overflow CVE Name: CAN-2002-0050	High	CyberNotes-2002-04
Microsoft ⁹⁵³	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.01, 5.01SP1&2, 5.5, 5.5SP1&2, 6.0	Internet Explorer Multiple Vulnerabilities CVE Names: CAN-2002-0022, CAN-2002-0023, CAN-2002-0024, CAN-2002-0025, CAN-2002-0026, CAN-2002-0027	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-04
Microsoft ⁹⁵⁴ <i>Microsoft re-releases bulletin⁹⁵⁵</i>	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.01, 5.01SP1&2, 5.5, 5.5SP1&2, 6.0	Internet Explorer VBScript Policy Violation CVE Name: CAN-2002-0052	Medium	CyberNotes-2002-04 CyberNotes-2002-06
Microsoft ⁹⁵⁶	Windows XP	Microsoft XML Core Services versions 2.6, 3.0, and 4.0	Windows XPXMLHTTP Sensitive Information CVE Name: CAN-2002-0057	Medium	CyberNotes-2002-04
Microsoft ⁹⁵⁷	Windows 95/98/ME/NT 4.0/2000	Outlook Express 5.5, 6.0	Outlook Express Non-existing Attachment	High	CyberNotes-2002-04
Microsoft ⁹⁵⁸	Windows NT 4.0	SQL Server 7.0 SP1-3 alpha, 7.0 SP1-3, 2000, 2000SP1-3	SQL Server OLE DB Provider Name Buffer Overflow CVE Name: CAN-2002-0056	High	CyberNotes-2002-04
Microsoft ⁹⁵⁹	Windows 2000	Windows 2000 Server, 2000 Server SP1& SP2	Windows 2000 Server Terminal Services Terminal Lock	Medium	CyberNotes-2002-04
Microsoft ⁹⁶⁰ <i>New versions of bulletin released^{961, 962, 963}</i> <i>Bulletin has been updated⁹⁶⁴</i>	Windows 95/98/NT 4.0/2000, XP	Windows 95, 98, 98SE, NT 4.0, NT 4.0 Server, Terminal Server Edition, 2000, XP	Windows Unchecked Buffer SNMP Service CVE Name: CAN-2002-0053	High	CyberNotes-2002-04 CyberNotes-2002-05 CyberNotes-2002-06 CyberNotes-2002-09
Microsoft ⁹⁶⁵ <i>Microsoft re-releases bulletin⁹⁶⁶</i>	Windows 95/98/ME/NT 4.0/2000, XP	All builds of the Microsoft VM up to and including build 3802	Microsoft Java Applet Browser Traffic Redirect CVE Names: CAN-2002-0058; CAN-2002-0076	High	CyberNotes-2002-05 CyberNotes-2002-06
Microsoft ⁹⁶⁷ <i>Microsoft re-releases bulletin⁹⁶⁸</i>	Windows 2000, XP	Exchange Server 2000 0.0, 2000 0.0 SP1&2, Advanced Server 0.0, 0.0 SP1&2, Professional 0.0, 0.0SP1&2, 2000 Server 0.0, 0.0SP1&2, XP Professional 0.0	Microsoft SMTP Service Malformed Data Remote Denial of Service CVE Name: CAN-2002-0055	Low	CyberNotes-2002-05 CyberNotes-2002-06
Microsoft ⁹⁶⁹ <i>Microsoft re-releases bulletin⁹⁷⁰</i>	Windows NT 4.0/2000	Exchange Server 5.5, 5.5SP1-4, 2000 Advanced Server 0.0, 0.0SP1&2, Datacenter Server 0.0, 0.0SP1&2, Professional 0.0, 0.0SP1&2, 2000 Server 0.0, 0.0SP1&2	Microsoft Windows SMTP Service Authentication CVE Name: CAN-2002-0054	Medium	CyberNotes-2002-05 CyberNotes-2002-06
Microsoft ⁹⁷¹	Windows NT 4.0/2000, XP	Microsoft IIS 4.0alpha, 4.0, 5.0, 5.1	Microsoft IIS Authentication	Medium	CyberNotes-2002-05
Microsoft ⁹⁷²	Windows NT 4.0	SQL Server 7.0, 7.0alpha, 7.0SP1-3, 7.0SP1-3 alpha	Microsoft SQL Server Buffer Overflow	High	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ⁹⁷³	Windows 98/SE/NT 4.0/2000	Windows NT Workstation 4.0, 4.0SP1-6a, Terminal Server 4.0, 4.0SP1-6a, Server 4.0, 4.0SP1-6a, Enterprise Server 4.0, 4.0SP1-6a, 2000 Terminal Services 0.0, 0.0SP1-2, 2000 Server 0.0, 0.0SP1-2, Professional 0.0, 0.0SP1-2, Datacenter Server 0.0, 0.0SP1-2, Advanced Server 0.0, 0.0SP1-2	Microsoft Windows User Shell Buffer Overflow CVE Name: CAN-2001-0070	High	CyberNotes-2002-05
Microsoft ⁹⁷⁴	Windows NT 4.0	Microsoft Windows NT Server 4.0, 4.0 SP1-6a	Windows NT Password Changing Bypass	Medium	CyberNotes-2002-06
Microsoft ⁹⁷⁵	Windows 95/98/ME/NT 4.0/2000, XP	MSN Messenger Service 3.6	MSN Messenger Message Spoofing	Medium	CyberNotes-2002-06
Microsoft ⁹⁷⁶	Windows 95/98/ME/NT 4.0/2000	Outlook 2002 0.0, Outlook Express 6.0	Outlook Multiple Vulnerabilities	High	CyberNotes-2002-06
Microsoft ⁹⁷⁷ <i>Microsoft releases patch⁹⁷⁸</i>	Windows NT 4.0/2000	Windows NT Workstation 4.0, 4.0SP1-6a; Terminal Server 4.0, 4.0SP1-6a; Server 4.0, 4.0SP1-6a; Enterprise Server 4.0, 4.0SP1-6a; 2000 Terminal Services 0.0, 0.0SP1-2; 2000 Server 0.0, 0.0SP1-2; 2000 Professional 0.0, 0.0SP1-2; 2000 Datacenter Server 0.0, 0.0SP1-2; 2000 Advanced Server 0.0, 0.0SP1-2	Windows 2000/NT 4.0 Privilege Elevation CVE Name: CAN-2002-0367	High	CyberNotes-2002-06 CyberNotes-2002-11
Microsoft ⁹⁷⁹	Windows NT 4.0/2000	Exchange Server 5.5, 5.5 SP1-4, Exchange Server 2000, 2000SP1&2; RSA Security SecurID 5.0	Microsoft Outlook Web Access with RSA SecurID Authentication Bypass	Medium	CyberNotes-2002-07
Microsoft ⁹⁸⁰	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0	Internet Explorer DYNsrc File Information Disclosure	Medium	CyberNotes-2002-07
Microsoft ⁹⁸¹	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0	Internet Explorer Cascading Style Sheet Sensitive Information	Medium	CyberNotes-2002-07
Microsoft ⁹⁸² <i>Bulletin has been revised⁹⁸³</i>	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0	Internet Explorer Known Local File Script Execution CVE Names: CAN-2002-0077, CAN-2002-0078	Medium High (High if arbitrary code can be executed)	CyberNotes-2002-07 CyberNotes-2002-08
Microsoft ⁹⁸⁴	Windows 95/98/ME/NT 4.0/2000, XP	Internet Explorer 6.0, Outlook 2000, 2002, Outlook Express 6.0	Microsoft Temporary Internet File Execution	High	CyberNotes-2002-07
Microsoft ⁹⁸⁵ <i>Updated Advisory released⁹⁸⁶</i>	Windows NT 4.0/2000, XP	Outlook 2002	Outlook 2002 HTML Mail Script Execution & Host(). SaveAs() File Creation	High	CyberNotes-2002-07 CyberNotes-2002-09
Microsoft ⁹⁸⁷	Windows 2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2	Windows 2000 DCOM Client Sensitive Information	Medium	CyberNotes-2002-07
Microsoft ⁹⁸⁸ <i>Microsoft releases revised bulletin⁹⁸⁹</i>	Windows NT 4.0/2000, XP	Windows 2000 Server, 2000 Advanced Server, 2000 Datacenter Server	Windows Group Policy File Block Policy CVE Name: CAN-2002-0051	Medium	CyberNotes-2002-07 CyberNotes-2002-08

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ⁹⁹⁰ <i>Microsoft updates bulletin</i> ⁹⁹¹	Windows NT 4.0/2000, XP	Windows NT 4.0 Workstation, 4.0 Server, 4.0 Server, Enterprise Edition, Terminal Server Edition, 2000 Professional, 2000 Server, 2000 Advanced Server, XP Professional	Windows Multiple UNC Provider Buffer Overflow CVE Name: CAN-2002-0151	High	CyberNotes-2002-07 CyberNotes-2002-08
Microsoft ⁹⁹²	Windows NT 4.0	BackOffice 4.0, 4.5	BackOffice Server Web Administration Login Bypass	Medium	CyberNotes-2002-08
Microsoft ⁹⁹³	Windows 2000	IIS 5.0	IIS CodeBrws. ASP File Extension Sensitive Information	Medium	CyberNotes-2002-08
Microsoft ⁹⁹⁴	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1SP1&2, 5.5, 6.0; Outlook 2000, 2002; Outlook Express 4.0, 5.0, 5.5, 6.0; Word 2000, 2000 SR1, SP1a, SR2, 2002	Microsoft VBScript ActiveX Word Object Denial of Service	Low	CyberNotes-2002-08
Microsoft ⁹⁹⁵	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.5, 5.5SP1&2, 6.0	Internet Explorer Dialog Origin Policy Bypass	High	CyberNotes-2002-08
Microsoft ⁹⁹⁶	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	Internet Explorer History List	High	CyberNotes-2002-08
Microsoft ⁹⁹⁷	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	Internet Explorer Unicode Character Denial of Service	Low	CyberNotes-2002-08
Microsoft ⁹⁹⁸	MacOS 7.0/8.0/9.0, MacOS X 10.x	Internet Explorer Macintosh Edition 5.1; Office 2001 For Macintosh SR1, Office 2001 For Macintosh, Office v. X; Outlook Express for MacOS 5.0-5.0.3; PowerPoint 98 for Mac; Excel v. X for Macintosh, 2001 for Macintosh; Entourage v. X for Macintosh, 2001 for Macintosh	Multiple Microsoft Products for MacOS File Vulnerabilities CVE Names: CAN-2002-0152, CAN-2002-0153	High	CyberNotes-2002-08
Microsoft ⁹⁹⁹ <i>Microsoft issues patch</i> ¹⁰⁰⁰	Office 2000, XP	<i>OfficeWeb Components 2000, 2002, Project 2000, 2002</i>	Office Web Component Clipboard Information Disclosure CVE Name: CAN-2002-0861	Medium	CyberNotes-2002-08 CyberNotes-2002-17
Microsoft ¹⁰⁰¹ <i>Microsoft issues patch</i> ¹⁰⁰²	Windows 2000, XP	<i>OfficeWeb Components 2000, 2002, Project 2000, 2002</i>	Office Web Component Local File CVE Name: CAN-2002-0860	Medium	CyberNotes-2002-08 CyberNotes-2002-17
Microsoft ¹⁰⁰³ <i>Microsoft issues patch</i> ¹⁰⁰⁴	Windows 2000, XP	<i>OfficeWeb Components 2000, 2002, Project 2002, Project Server 2002</i>	Office Web Components Multiple Vulnerabilities CVE Name: CAN-2002-0860	Medium	CyberNotes-2002-08 CyberNotes-2002-17
Microsoft ¹⁰⁰⁵ <i>Microsoft issues patch</i> ¹⁰⁰⁶	Windows 2000, XP	<i>OfficeWeb Components 2000, 2002, Project 2002, Project Server 2002</i>	Office Web Components Active Script Execution CVE Name: CAN-2002-0727	High	CyberNotes-2002-08 CyberNotes-2002-17
Microsoft ¹⁰⁰⁷	Windows NT 4.0/2000	SQL Server 7.0, 2000	SQL Server Buffer Overflow CVE Name: CAN-2002-0154	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-08
Microsoft ¹⁰⁰⁸	Windows 2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2	Windows 2000 Denial of Service	Low	CyberNotes-2002-08
Microsoft ¹⁰⁰⁹	Windows 2000	Windows 2000 Terminal Services, 2000SP1&2	Windows Terminal Server Group Policy Bypass	Medium	CyberNotes-2002-08
Microsoft ¹⁰¹⁰	Windows NT	Baseline Security Analyzer 1.0	Baseline Security Analyzer Plaintext File	Medium	CyberNotes-2002-09

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹⁰¹¹	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1 SP1&2, 5.5, 5.5SP1&2, 6.0	Internet Explorer Recursive Denial of Service	Low	CyberNotes-2002-09
Microsoft ¹⁰¹²	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.5, 5.5SP1, 6.0	Internet Explorer Self-Referential Object Denial of Service	Low	CyberNotes-2002-09
Microsoft ¹⁰¹³	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 6.0, Outlook Express 6.0	Internet Explorer/ Outlook Express XBM Denial of Service	Low	CyberNotes-2002-09
Microsoft ¹⁰¹⁴	Windows	Outlook 2000, 2002	Outlook E-mail Editor Script Execution CVE Name: CAN-2002-1056	High	CyberNotes-2002-09
Microsoft ¹⁰¹⁵	Window 95/98/ME/NT 4.0/2000	Internet Explorer 5.01, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0	Multiple Microsoft Internet Explorer Vulnerabilities CVE Names: CAN-2002-0188, CAN-2002-0189, CAN-2002-0190, CAN-2002-0191, CAN-2002-0192, CAN-2002-0193	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-10
Microsoft ¹⁰¹⁶ <i>Microsoft updates bulletin¹⁰¹⁷</i>	Multiple	MSN Chat Control	MSN Chat Control Remote Buffer Overflow CVE Name: CAN-2002-0155	High	CyberNotes-2002-10 CyberNotes-2002-12
Microsoft ¹⁰¹⁸	Windows 95/98/ME/NT 4.0/2000	MSN Messenger Service 1.0, 2.0, 2.2, 3.0, 3.6, 4.0, 4.5, 4.6	MSN Messenger Font Tag Denial Of Service	Low	CyberNotes-2002-10
Microsoft ¹⁰¹⁹	Windows 95/98/ME/NT 4.0/2000	Excel 2002	Excel 2002 XML Stylesheet Arbitrary Code Execution	High	CyberNotes-2002-11
Microsoft ¹⁰²⁰	Windows 2000	Exchange Server 2000, 2000 SP1&2	Exchange 2000 Malformed Mail Attribute Remote Denial of Service CVE Name: CAN-2002-0368	Low	CyberNotes-2002-11
Microsoft ¹⁰²¹	Windows	MSDE 1.0, SQL Server 2000 Desktop Engine	MSDE/SQL Server Null Password	High	CyberNotes-2002-11
Microsoft ¹⁰²²	Windows 95/98/ME/NT 4.0/2000, XP	MSN Messenger Service 1.0, 2.0, 2.2, 3.0, 3.6, 4.0, 4.5, 4.6	MSN Messenger Malformed Invite Request Remote Denial of Service	Low	CyberNotes-2002-11
Microsoft ¹⁰²³	Windows 2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, Windows 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Server, 2000 Server SP1&2	Microsoft Active Directory Denial of Service	Low	CyberNotes-2002-11
Microsoft ¹⁰²⁴	Windows	.NET Framework 1.0 SP1, 1.0	Microsoft ASP.NET StateServer Buffer Overflow CVE Name: CAN-2002-0369	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-12
Microsoft ¹⁰²⁵ <i>Microsoft updates bulletin¹⁰²⁶</i>	Windows NT 4.0/2000	IIS 4.0, 5.0	Microsoft IIS ISAPI Extension Buffer Overflow CVE Name: CAN-2002-0364	High	CyberNotes-2002-12 CyberNotes-2002-14
Microsoft ¹⁰²⁷ <i>Microsoft issues patch¹⁰²⁸</i>	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0; Proxy Server 2.0; ISA Server 2000	Multiple Microsoft Product Gopher Client Buffer Overflows CVE Names: CAN-2002-0371, CAN-2002-0646	High	CyberNotes-2002-12 CyberNotes-2002-17
Microsoft ¹⁰²⁹	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2, 6.0	Internet Explorer Cross-Site Scripting	High	CyberNotes-2002-12

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹⁰³⁰	Windows NT 4.0/2000	SQL Server 2000, 2000 SP1&2	Microsoft SQL Server Vulnerabilities CVE Name: CAN-2002-0186, CAN-2002-0187	High	CyberNotes-2002-12
Microsoft ¹⁰³¹	Windows NT 4.0/2000, XP	Visual Basic .NET, Visual C# .NET, Visual C++.Net, Visual Studio .NET Academic Edition, Enterprise Architect Edition, Enterprise Developer Edition, Professional Edition, Trial Edition	Visual Studio .NET Korean Version Nimda Infected	Medium	CyberNotes-2002-12
Microsoft ¹⁰³² <i>Revised patch issued¹⁰³³</i>	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2, NT Enterprise Server 4.0, NT Enterprise Server 4.0 SP1-6a, NT Server 4.0, NT Server 4.0 SP1-6a, NT Terminal Server 4.0, NT Terminal Server 4.0 SP1-6a, NT Work-station 4.0, NT Work-station 4.0 SP1-6a, XP 64-bit Edition, XP Home, XP Professional	Windows 2000 Remote Access Service Buffer Overflow CVE Name: CAN-2002-0366	High	CyberNotes-2002-12 CyberNotes-2002-14
Microsoft ¹⁰³⁴	Windows 2000	Commerce Server 2000, 2000 SP1&2	Commerce Server Multiple Vulnerabilities CVE Names: CAN-2002-0050, CAN-2002-0620, CAN-2002-0621, CAN-2002-0622, CAN-2002-0623	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-13
Microsoft ¹⁰³⁵	Windows 95/98/ME/NT 4.0/2000, XP	Excel 2000, 2000 SR1, 2000 SP1, 2002, 2002 SP2; Office 2000; Office XP	Excel Multiple Vulnerabilities CVE Names: CAN-2002-0616, CAN-2002-0617, CAN-2002-0618, CAN-2002-0619	High	CyberNotes-2002-13
Microsoft ¹⁰³⁶	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 6.0	Internet Explorer Denial of Service	Low	CyberNotes-2002-13
Microsoft ¹⁰³⁷	Windows NT 4.0/2000	Microsoft JET 4.0, 4.0 SP1-SP5; SQL Server 2000, 2000 SP1&2	SQL Server 2000 OpenData Source Buffer Overflow	High	CyberNotes-2002-13
Microsoft ¹⁰³⁸	Windows NT 4.0/2000	SQL Server 2000, SQL Server 2000 SP1&2	SQL Server 2000 PWDEncrypt Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-13
Microsoft ¹⁰³⁹ <i>Bulletin updated¹⁰⁴⁰</i>	Windows 95/98/ME/NT 4.0/2000, XP	Windows Media Player XP, 6.4, 7.1	Windows Media Player Multiple Vulnerabilities CVE Names: CAN-2002-0372, CAN-2002-0373, CAN-2002-0615	High	CyberNotes-2002-13 CyberNotes-2002-16
Microsoft ¹⁰⁴¹ <i>Microsoft issues patch¹⁰⁴²</i>	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2, 6.0	Internet Explorer Universal Cross Domain Scripting CVE Name: CAN-2002-0723	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-14 CyberNotes-2002-17

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹⁰⁴³	Windows	SQL Server 2000 all editions, Desktop Engine (MSDE) 2000	Multiple SQL Server Vulnerabilities CVE Names: CAN-2002-0624, CAN-2002-0641, CAN-2002-0642	High	CyberNotes-2002-14
Microsoft ¹⁰⁴⁴	Windows NT 4.0/2000	SQL Server 7, including Microsoft Data Engine 1.0 (MSDE 1.0), SQL Server 2000	SQL Server Installation Process Password Storage CVE Name: CAN-2002-0643	Medium	CyberNotes-2002-14
Microsoft ¹⁰⁴⁵	Windows NT 4.0/2000	Exchange Server 5.5, 5.5 SP1&2, IIS 4.0, 5.0	IIS SMTP Service Encapsulated SMTP Address	Medium	CyberNotes-2002-15
Microsoft ¹⁰⁴⁶	Windows NT 4.0/2000	Exchange Server 5.5, 5.5 SP1-4	Microsoft Exchange Server IMC EHLO Response Buffer Overflow CVE Name: CAN-2002-0698	High	CyberNotes-2002-15
Microsoft ¹⁰⁴⁷	Windows	Meta-directory Services 2.2	Microsoft Metadirectory Services Remote LDAP Client Administration CVE Name: CAN-2002-0697	High	CyberNotes-2002-15
Microsoft ¹⁰⁴⁸	Windows 95/98/NT 4.0/2000, MacOS 7.0/8.0/ 8.1/ 8.5/ 8.6/9.0, MacOS X 10.0, 10.1	Outlook Express 4.0, 4.27.3110, 4.72.2106, 4.72.3120, 4.72.3612, 5.0, 5.5, 6.0, Outlook Express for MacOS 4.5, 5.0, 5.0.1-5.0.3	Outlook Express SMTP Over TLS Information Disclosure	Medium	CyberNotes-2002-15
Microsoft ¹⁰⁴⁹	Windows 95/98/NT 4.0/2000	Outlook Express 5.0, 5.5, 6.0	Microsoft Outlook Express Spoofable File Extensions	Medium	CyberNotes-2002-15
Microsoft ¹⁰⁵⁰	Windows NT 4.0/2000	SQL Server 2000 , 2000 SP1&2, SQL Server 2000 Desktop Engine	Microsoft SQL Server 2000 Database Consistency Checkers Buffer Overflow & SQL Server 2000 Replication Stored Procedures Injection CVE Names: CAN-2001-0644, CAN-2002-0645	High	CyberNotes-2002-15
Microsoft ¹⁰⁵¹	Windows NT 4.0/2000	SQL Server 2000, 2002 SP1&2	Microsoft SQL Server 2000 Multiple Vulnerabilities CVE Names: CAN-2002-0649, CAN-2002-0650	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-15
Microsoft ¹⁰⁵²	Windows 2002	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2	Windows 2000 Narrator Password Disclosure	Medium	CyberNotes-2002-15
Microsoft ¹⁰⁵³	Windows NT 4.0/2000, XP	Content Management Server 2001, Content Management Server 2001 SP1	Multiple Microsoft Content Management Server 2001 Vulnerabilities CVE Names: CAN-2002-0700, CAN-2002-0718, CAN-2002-0719	High	CyberNotes-2002-16
Microsoft ¹⁰⁵⁴	Windows 2000	Exchange Server 2000, Exchange Server 2000 SP1&2	Exchange 2000 License Allocation Denial of Service	Low	CyberNotes-2002-16
Microsoft ¹⁰⁵⁵	Windows 2000	Exchange Server 2000, Exchange Server 2000 SP1&2	Exchange 2000 Multiple MSRPC Denial of Service	Low	CyberNotes-2002-16
Microsoft ¹⁰⁵⁶	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0	Internet Explorer Invalid SSL Certificate Chain	Medium	CyberNotes-2002-16

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹⁰⁵⁷	Windows 98/ME/NT 4.0/2000, XP	Internet Explorer 6.0, Office Web Components 9, 10, Office XP	Office XP/Internet Explorer	High	CyberNotes-2002-16
Microsoft ¹⁰⁵⁸	Windows 98/NT 4.0/2000, XP	MDAC 1.5, 2.0, 2.1 Upgrade, 2.1 Clean, 2.1 2.4202.3 (GA) clean, 2.1 2.4202.3 (GA), 2.1.1 .3711.11 (GA), 2.5, 2.5 SP1&2, 2.5 RTM, 2.6, 2.6 SP1&2, 2.6 RTM, 2.7, 2.7 RTM Refresh	Microsoft Data Access Components T-SQL Buffer Overflow CVE Name: CAN-2002-0695	High	CyberNotes-2002-16
Microsoft ¹⁰⁵⁹	Windows	Outlook Express 6.0	Microsoft Outlook Express XML File Attachment Script Execution	High	CyberNotes-2002-16
Microsoft ¹⁰⁶⁰	Windows NT 4.0/2000	SQL Server 2000, SQL Server 2000 SP1&2	SQL Server Remote Buffer Overflow	High	CyberNotes-2002-16
Microsoft ¹⁰⁶¹	Windows 2000	Windows 2000 Advanced Server, SP1&2, 2000 Datacenter Server, SP1&2, 2000 Professional, SP1&2, 2000 Server, SP1&2, 2000 Terminal Services, SP1&2	Microsoft Windows 2000 Insecure Default File Permissions	Medium	CyberNotes-2002-16
Microsoft ¹⁰⁶² <i>Microsoft releases bulletin¹⁰⁶³</i>	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1&2, Datacenter Server, SP1&2, Professional, SP1&2, 2000 Server, SP1&2, 2000 Server Japanese Edition, 2000 Terminal Services, SP1&2, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Windows XP, 64-bit Edition, Home, Professional	Microsoft Windows Message Subsystem Design Error	Medium	CyberNotes-2002-16 CyberNotes-2002-25
Microsoft ¹⁰⁶⁴	Windows NT	Windows 2000 Terminal Services SP1&2, 2000 Terminal Services	Microsoft Windows Terminal Services Denial Of Service	Low	CyberNotes-2002-16
Microsoft ¹⁰⁶⁵	Windows 95/98/ME/NT 4.0/2000, XP, MacOS 7.0/7.0.1/ 7.1/7.1.2/ 7.5.1/7.5.2/ 7.5.3/7.6/ 7.6.1/8.0, Unix	Windows Media Player XP, 6.3, 6.4, 7.0, 7.1	Windows Media Player Filename Buffer Overflow	Medium	CyberNotes-2002-16
Microsoft ¹⁰⁶⁶	Windows NT 4.0/2000	2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2, 2000 Terminal Services, 2000 Terminal Services SP1&2	Windows NTFS Incorrect Hard Link Auditing CVE Name: CAN-2002-0725	Medium	CyberNotes-2002-17
Microsoft ¹⁰⁶⁷	Windows NT 4.0/2000, XP	2000 Advanced Server, 2000 Advanced Server SP1-3, 2000 Datacenter Server, 2000 Datacenter Server SP1-3, 2000 Professional, 2000 Professional SP1-3, 2000 Server, 2000 Server SP1-3, 2000 Terminal Services, 2000 Terminal Services SP1-3	Windows 2000 Network Connection Manager Privilege Elevation CVE Name: CAN-2002-0720	Medium	CyberNotes-2002-17
Microsoft ¹⁰⁶⁸	Windows NT 4.0/2000	Data Engine 1.0, 2000, SQL Server 7.0, SQL Server 7.0 SP1-4, SQL Server 2000, SQL Server 2000 SP1&2	Microsoft SQL Agent Jobs Privilege Elevation	Medium	CyberNotes-2002-17

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹⁰⁶⁹	Windows NT 4.0/2000	Data Engine 1.0, 2000, SQL Server 7.0. SQL Server 7.0 SP1-4, SQL Server 2000, SQL Server 2000 SP1&2	Microsoft SQL Server Extended Stored Procedure Privilege Elevation CVE Name: CAN-2002-0721	High	CyberNotes-2002-17
Microsoft ¹⁰⁷⁰	Windows	DirectX Files Viewer	DirectX Files Viewer Remote Buffer Overflow	High	CyberNotes-2002-17
Microsoft ¹⁰⁷¹	Windows	File Transfer Manager	Microsoft File Transfer Manager ActiveX Control Buffer Overflow & Arbitrary File Upload	Medium/High (High if arbitrary code is executed)	CyberNotes-2002-17
Microsoft ¹⁰⁷²	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 4.0, 4.0.1, 4.0.1 SP2, 5.0, 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0	Internet Explorer XML Datasource Applet	Medium	CyberNotes-2002-17
Microsoft ¹⁰⁷³	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2, 6.0	Internet Explorer Web Folder HTML Injection	High	CyberNotes-2002-17
Microsoft ¹⁰⁷⁴	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2, 6.0	Internet Explorer Multiple Vulnerabilities CVE Names: CAN-2002-0691, CAN-2002-0647, CAN-2002-0648, CAN-2002-0722	Medium/High (High if arbitrary code is executed)	CyberNotes-2002-17
Microsoft ¹⁰⁷⁵	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	Internet Explorer Script Execution	High	CyberNotes-2002-17
Microsoft ¹⁰⁷⁶	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	Microsoft Internet Explorer Java Logging Executable Code	High	CyberNotes-2002-17
Microsoft ¹⁰⁷⁷	Windows 95/98/ME/ NT 4.0/2000, XP	TSAC ActiveX Control	TSAC ActiveX Control Buffer Overflow CVE Name: CAN-2002-0726	High	CyberNotes-2002-17
Microsoft ¹⁰⁷⁸	Windows 2000	Windows 2000 Terminal Services, Terminal Services SP1-SP3	Terminal Services Inactive Console Screensaver Lock Failure	Medium	CyberNotes-2002-17
Microsoft ¹⁰⁷⁹	Windows NT 4.0/2000, XP	Windows NT 4.0 Server, NT 4.0 Work-station, NT 4.0 Server, Terminal Server Edition, 2000 Professional, 2000 Server, 2000 Advanced Server, XP Professional	Network Share Provider SMB Request Buffer Denial of Service CVE Name: CAN-2002-0724	Low	CyberNotes-2002-17
Microsoft ¹⁰⁸⁰ <i>Microsoft issues bulletin¹⁰⁸¹</i>	Windows XP	Windows XP Home, XP Professional, Internet Explorer 6.0	Microsoft Windows XP HCP URI Handler Abuse CVE Name: CAN-2002-0974	Medium	CyberNotes-2002-17 CyberNotes-2002-21
Microsoft ¹⁰⁸²	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	Internet Explorer HTML Same Origin Policy Violation	Medium	CyberNotes-2002-18
Microsoft ¹⁰⁸³	Windows NT 4.0/2000	SQL Server 2000, 2000 SP1&2	SQL Server Stored Procedure Low Privilege	Medium	CyberNotes-2002-18
Microsoft ¹⁰⁸⁴	Windows	Visual FoxPro 6.0	Microsoft Visual FoxPro 6.0 Automatic Application Execution CVE Name: CAN-2002-0696	High	CyberNotes-2002-18

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹⁰⁸⁵	Windows 95/98/MT/ NT 4.0/2000, XP	Windows 2000 Advanced Server, Advanced Server SP1-SP3, 2000 Datacenter Server, Datacenter Server SP1-SP3, 2000 Professional, Professional SP1-SP3, Server, Server SP1-SP3, 2000 Terminal Services, Terminal Services SP1-SP3, Windows 95, 98, 98SE, 98ME, NT Enterprise Server 4.0, Enterprise Server 4.0 SP1-SP6a, NT Server 4.0, Server 4.0 SP1-SP6a, NT Terminal Server 4.0, Terminal Server 4.0 SP1-SP6a, NT Workstation 4.0, Workstation 4.0 SP1-SP6a, XP 64-bit Edition, XP Home, XP Professional	Microsoft ActiveX Certificate Enrollment Control Certificate Destruction CVE Name: CAN-2002-0699	Medium	CyberNotes-2002-18
Microsoft ¹⁰⁸⁶ <i>Microsoft updates patch¹⁰⁸⁷</i>	Windows 98/ME/NT 4.0/2000, XP, Mac OS 8.1 to 9.x, MacOS X	Windows 98, ME, NT 4.0, NT 4.0 Terminal Server Edition, 2000, XP, Office for Mac, Internet Explorer for Mac, Outlook Express for Mac	Microsoft Certificate Validation CVE Name: CAN-2002-0862	High	CyberNotes-2002-18 CyberNotes-2002-24
Microsoft ¹⁰⁸⁸ <i>Microsoft issues bulletin¹⁰⁸⁹</i>	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS	Word 2000, 2000 SR1a, 2000 SR1&2, Word 2002, Word 95, Word 97, 97 SR1&2, Word 98, <i>Word 2001 for Macintosh Word 98 for Macintosh, Word 98 Japanese Version, Excel 2002</i>	Word /Excel INCLUDE TEXT Document CVE Name: CAN-2002-1143	High	CyberNotes-2002-18 CyberNotes-2002-21
Microsoft ¹⁰⁹⁰	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0, 5.0 for Windows 95/98/ NT 4.0/2000, 5.0.1, 5.0.1 SP1&2, 5.0.1 for Windows 95/98/NT 4.0/2000, 5.5, 5.5 SP1&2, 5.5 preview, 6.0	Internet Explorer IFrame/Frame Cross-Site/Zone Script Execution	High	CyberNotes-2002-19
Microsoft ¹⁰⁹¹	Windows	JVM 1.1	Multiple JVM Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-19
Microsoft ¹⁰⁹²	Windows NT 4.0/2000	NetMeeting 3.0.1 4.4.3385	NetMeeting Local Session Hijacking	High	CyberNotes-2002-19
Microsoft ¹⁰⁹³	Windows 95/98/NT 4.0/2000	Outlook Express 5.01, 5.0, 5.5, 6.0	Outlook Express Link Denial of Service	Low	CyberNotes-2002-19
Microsoft ¹⁰⁹⁴	Windows 95/98/NT 3.51/4.0/ 2000	Virtual Machine 2000 Series, 3000 Series, 3100 Series, 3188, 3200 Series, 3300 Series, 3802 Series, 3805 Series	Virtual Machine Multiple Vulnerabilities CVE Names: CAN-2002-0865, CAN-2002-0866, CAN-2002-0867	Low/High (High if arbitrary code is executed)	CyberNotes-2002-19
Microsoft ¹⁰⁹⁵	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, Windows 2000 Advanced Server SP1-3, Datacenter Server, Datacenter Server SP1-3, 2000 Professional, 2000 Professional SP1-3, 2000 Server, 2000 Server SP1-3, Terminal Services, Terminal Services SP1-3, NT Terminal Server 4.0, Terminal Server 4.0 SP1-6a, XP 64-bit Edition, XP 64-bit Edition SP1, XP Home, XP Home SP1, XP Professional, XP Professional SP1	Microsoft Windows RDP Vulnerabilities CVE Names: CAN-2002-0863, CAN-2002-0864	Low/ Medium (Medium if sensitive information is obtained)	CyberNotes-2002-19

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹⁰⁹⁶	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, Windows 2000 Advanced Server SP1-3, Datacenter Server, Datacenter Server SP1-3, 2000 Professional, 2000 Professional SP1-3, 2000 Server, 2000 Server SP1-3, Terminal Services, Terminal Services SP1-3, NT Terminal Server 4.0, Terminal Server 4.0 SP1-6a, XP 64-bit Edition, XP 64-bit Edition SP1, XP Home, XP Home SP1, XP Professional, XP Professional SP1	Windows 2000/NT/XP 16-bit Application Permission Bypass	Medium	CyberNotes-2002-19
Microsoft ¹⁰⁹⁷	Windows NT 4.0/2000	Data Engine 1.0, 2000; SQL Server 7.0, 7.0 SP1-SP4, 2000, 2000 SP1&2	Multiple Microsoft SQL Server Vulnerabilities CVE Names: CAN-2002-1123, CAN-2002-1137, CAN-2002-1138	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Microsoft ¹⁰⁹⁸	Windows 2000, XP	FrontPage Server Extensions 2000, 2002, Windows 2000 Advanced Server, 2000 Advanced Server SP1-SP3, 2000 Professional, 2000 Professional SP1-SP3, 2000 Server, 2000 Server SP1-SP3, Windows XP Home, XP Home SP1, XP Professional, XP Professional SP1	Microsoft FrontPage Server Extensions SmartHTML Buffer Overflow CVE Name: CAN-2002-0692	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Microsoft ¹⁰⁹⁹	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1&2, 5.0.1 for Windows NT 4.0, 98, 95, 2000, 5.5, 5.5 SP1&2, 5.5 preview, 6.0, 6.0SP1	Internet Explorer Document Reference	High	CyberNotes-2002-20
Microsoft ¹¹⁰⁰	Windows	Internet Explorer 6.0 SP1	Microsoft Internet Explorer URI Handler Restriction Circumvention	Medium	CyberNotes-2002-20
Microsoft ¹¹⁰¹	Windows 98/ME/NT 4.0/2000, XP	Internet Explorer 6.0, 6.0 SP1	Microsoft Internet Explorer SSL Certificate Expiration	Medium	CyberNotes-2002-20
Microsoft ¹¹⁰²	Windows NT 4.0/2000, XP	Microsoft Services for Unix 3.0	Multiple Microsoft Services for Unix 3.0 Interix SDK CVE Names: CAN-2002-0391, CAN-2002-1140, CAN-2002-1141	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Microsoft ¹¹⁰³	Windows	Virtual Machine 2000 Series, 3000 Series, 3100 Series, 3188, 3200 Series, 3300 Series, 3802 Series, 3805 Series	Microsoft Virtual Machine Unauthorized ODBC Data Access	Medium	CyberNotes-2002-20
Microsoft ¹¹⁰⁴	Windows 2000, XP	Windows 2000 Advanced Server, 2000 Advanced Server SP1-SP3, 2000 Datacenter Server, 2000 Datacenter Server SP1-SP3, 2000 Professional, 2000 Professional SP1-SP3, 2000 Server, 2000 Server SP1-SP3, 2000 Terminal Services, 2000 Terminal Services SP1-SP3, XP Home, XP Home SP1, XP Professional, XP Professional SP1	Microsoft PPTP Server Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹¹⁰⁵	Windows 98/ME/NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, 98, 98 a/b/j, 98SE, ME, NT Server 4.0, NT Server 4.0 SP1-SP6a, NT Terminal Server 4.0, alpha, SP1-SP6a, NT Work-station 4.0, 4.0 SP1-SP6a, Windows XP, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	Microsoft Windows Help Facilities CVE Names: CAN-2002-0693, CAN-2002-0694	High	CyberNotes-2002-20
Microsoft ¹¹⁰⁶	Windows 98/ME, XP	Windows 98 With Plus! Pack, Windows ME , XP Home SP1, XP Home	Microsoft Windows 98/ME/XP File Decompression Vulnerabilities CVE Names: CAN-2002-0370, CAN-2002-1139	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Microsoft ¹¹⁰⁷	Windows 95/98/ME/ NT 4.0/2000, XP	Word 2000, Word 2000 SR1&1a, Word 2000 SP2, Word 2002, Word 2002 SP1, Word 95, Word 97, Word 97 SR1&2	Microsoft Word INCLUDE PICTURE Document Sharing File Disclosure	Medium	CyberNotes-2002-20
Microsoft ¹¹⁰⁸	Windows NT 4.0/2000, XP	Content Management Server 2001, 2001 SP1	Content Management Server 2001 Cross-Site Scripting	High	CyberNotes-2002-21
Microsoft ¹¹⁰⁹	Windows NT 4.0/2000	Data Engine 1.0, 2000, SQL Server 7.0, SQL Server 7.0 SP1-SP4, SQL Server 2000, SQL Server 2000 SP1&2	Microsoft SQL Server Web Task Stored Procedure Privilege Escalation CVE Name: CAN-2002-1145	Medium	CyberNotes-2002-21
Microsoft ¹¹¹⁰	Windows 2000	IIS 5.0	IIS .IDC Cross-Site Scripting	High	CyberNotes-2002-21
Microsoft ¹¹¹¹	Windows 2000, XP	IIS 5.0, 5.1	IIS Malformed HTTP HOST Remote Denial of Service	Low	CyberNotes-2002-21
Microsoft ¹¹¹²	Windows 95/98/ME NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2, 6.0	Internet Explorer Unauthorized DOM Access	Medium	CyberNotes-2002-21
Microsoft ¹¹¹³	Windows 95/98/NT 4.0/2000, XP	Outlook Express 5.5, 6.0	Outlook Express S/MIME Buffer Overflow CVE Name: CAN-2002-1179	High	CyberNotes-2002-21
Microsoft ¹¹¹⁴	Windows 95/98/NT 4.0/2000, XP	TSAC ActiveX Control	Microsoft TSAC Cross-Site Scripting	High	CyberNotes-2002-21
Microsoft ¹¹¹⁵	Windows 2000, XP	Windows 2000 Advanced Server, Advanced Server SP1&2, 2000 Datacenter Server, Datacenter Server SP1&2, 2000 Professional, Professional SP1&2, 2000 Server, 2000 Server SP1&2, 2000 Terminal Services, Terminal Services SP1&2, XP Home, XP Professional	Windows 2000/XP Full Event Log Administrative Alert	Medium	CyberNotes-2002-21
Microsoft ¹¹¹⁶	Windows 2000	Windows 2000 Terminal Services, Terminal Services SP1-SP3, 2000 Server, Server SP1-SP3, 2000 Professional, Professional SP1-SP3, 2000 Datacenter Server, Datacenter Server SP1-SP3, 2000 Advanced Server, Advanced Server SP1-SP3	Windows 2000 NetDDE Privilege Escalation	Medium	CyberNotes-2002-21
Microsoft ¹¹¹⁷	Windows XP	Windows XP Professional	Windows XP System Restore Directory Insecure Access Control	Medium	CyberNotes-2002-21

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹¹¹⁸	Windows 2000, XP	2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	Microsoft PPTP Buffer Overrun CVE Name: CAN-2002-1214	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-22
Microsoft ¹¹¹⁹	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0	Internet Explorer Document. Write() Zone Bypass	High	CyberNotes-2002-22
Microsoft ¹¹²⁰	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2, 6.0	Multiple Microsoft Internet Explorer Cached Objects Zone Bypass	High	CyberNotes-2002-22
Microsoft ¹¹²¹	Windows NT 4.0/2000, XP	Internet Information Service (IIS) 4.0, 5.0, 5.1	Internet Information Service Vulnerabilities CVE Names: CAN-2002-0869, CAN-2002-1180, CAN-2002-1181, CAN-2002-1182	Low/ High (High if arbitrary code can be executed)	CyberNotes-2002-22
Microsoft ¹¹²²	Windows 2000	Windows 2000 Advanced Server, SP1&2, 2000 Datacenter Server, SP1&2, 2000 Professional, SP1&2, 2000 Server, SP1&2, 2000 Terminal Services, SP1&2	Microsoft Windows 2000 SNMP Printer Query Denial of Service	Low	CyberNotes-2002-22
Microsoft ¹¹²³	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a	Microsoft Windows 2000 / NT Path Precedence CVE Name: CAN-2002-1184	Medium	CyberNotes-2002-22
Microsoft ¹¹²⁴	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, 2000 SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	Windows 2000 RPC Service Remote Denial of Service	Low	CyberNotes-2002-22
Microsoft ¹¹²⁵	Windows, Unix	Windows Media Player 6.3 Solaris	Windows Media Player World Writeable Executables	Medium	CyberNotes-2002-22
Microsoft ¹¹²⁶	Windows 95/98/NT 4.0/2000	JVM 1.1	Microsoft JVM Package Multiple Vulnerabilities	Low/ Medium/ High (Low if a Denial of Service, Medium if sensitive information can be obtained, and High if arbitrary code can be executed)	CyberNotes-2002-23
Microsoft ¹¹²⁷	Windows NT 4.0/2000	SQL Server 6.0, 6.5, 7.0, 7.0 SP1-SP4, SQL Server 2000, 2000 SP1&2	SQL Server Login Weak Password Encryption	Medium	CyberNotes-2002-23
Microsoft ¹¹²⁸	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0, 5.0 for Windows 95/98/ 2000, 5.0 for Windows NT 4.0, 5.0.1, 5.0.1 SP1&2, 5.0.1 for Windows 95/98/ 2000, 5.0.1 for Windows NT 4.0, 5.5, 5.5 SP1&2, Internet Explorer 6.0, 6.0SP1	Internet Explorer IFRAME dialog Arguments	High	CyberNotes-2002-24
Microsoft ¹¹²⁹	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0, 6.0 SP1; MDAC 2.1, 2.5, 2.6	Microsoft Data Access Components RDS Buffer Overflow CVE Name: CAN-2002-1142	High	CyberNotes-2002-24

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Microsoft ¹¹³⁰	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0, 6.0 SP1	Multiple Internet Explorer Vulnerabilities CVE Names: CAN-2002-1185, CAN-2002-1186, CAN-2002-1187, CAN-2002-1188, CAN-2002-1254, CAN-2002-1217	Low/ Medium/High Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	CyberNotes-2002-24
Microsoft ¹¹³¹	Multiple	Virtual Machine 3802 Series, 3805 Series	Microsoft Java Virtual Machine Bytecode Verifier	High	CyberNotes-2002-24
Microsoft ¹¹³²	Windows 95/98/ME/ NT 4.0/2000, XP	2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, Windows 95, 95 SR2, 98, 98SE, ME, NT Enterprise Server 4.0 SP1-SP6a, NT Server 4.0 SP1-SP6a, NT Terminal Server 4.0 SP1-SP6a, NT Work-station 4.0 SP1-SP6a, XP Home SP1, XP Professional SP1	Java Virtual Machine Multiple Vulnerabilities CVE Names: CAN-2002-1254, CAN-2002-1257, CAN-2002-1258, CAN-2002-1259, CAN-2002-1260, CAN-2002-1261, CAN-2002-1263	Low/ Medium/High (Medium if sensitive information can be obtained and High if control can be obtained over the system)	CyberNotes-2002-25
Microsoft ¹¹³³	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 6.0	Internet Explorer Object Caching CVE Name: CAN-2002-1262	High	CyberNotes-2002-25
Microsoft ¹¹³⁴	Windows 98/ME/NT 4.0/2000, XP	Outlook 2002, 2002 SP1&SP2	Outlook 2002 E-mail Header Processing Denial of Service CVE Name: CAN-2002-1255	Low	CyberNotes-2002-25
Microsoft ¹¹³⁵	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, XP 64-bit Edition, XP Home, XP Professional	Windows SMB Signing CVE Name: CAN-2002-1256	Medium	CyberNotes-2002-25
Microsoft ¹¹³⁶	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, XP Home, XP Home SP1, XP Professional, XP Professional SP1	Windows 2000/XP WM_TIMER Message Handling CVE Name: CAN-2002-1230	High	CyberNotes-2002-25
Microsoft ¹¹³⁷	Windows XP	Windows XP Home, XP Home SP1, Professional, Professional SP1	Windows XP Fast User Switching Process Viewing	Medium	CyberNotes-2002-25
Microsoft ¹¹³⁸	Windows XP	Windows XP Home, XP Home SP1, XP Professional, XP Professional SP1	Microsoft Windows XP Wireless LAN Information Disclosure	Medium	CyberNotes-2002-25
Microsoft ¹¹³⁹	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0, 6.0 SP1	Microsoft Internet Explorer Dialog Style Same Origin Policy Bypass	High	CyberNotes-2002-25.
Microsoft ^{1140, 1141} <i>Updated bulletin released¹¹⁴²</i>	Windows NT 4.0/2000, XP	Microsoft IIS 4.0, 5.0, 5.1; Cisco Building Broadband Service Manager 4.x, 5.x, Call Manager 3.0-3.2, Unity Server 2.0-2.4	Microsoft IIS Multiple Vulnerabilities CVE Names: CAN-2002-0071, CAN-2002-0072, CAN-2002-0073, CAN-2002-0074, CAN-2002-0075, CAN-2002-0079, CAN-2002-0147, CAN-2002-0148, CAN-2002-0149, CAN-2002-0150	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-08 CyberNotes-2002-10

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
MiniBB ¹¹⁴³	Multiple	MiniBB 1.2	MiniBB Cross-Site Scripting	High	CyberNotes-2002-09
Mirabilis ¹¹⁴⁴	Windows 95/98/ME/NT 4.0/2000	ICQ 2000.0b Build 3278, 2000.0A	ICQ Remote Buffer Overflow	Low/High (High if arbitrary code is executed)	CyberNotes-2002-01
Mirabilis ¹¹⁴⁵	MacOS X 10.0-10.0.4 10.1-10.1.2	ICQ For MacOS X 2.6X Beta	ICQ For MacOS X Denial Of Service	Low	CyberNotes-2002-03
Mirabilis ¹¹⁴⁶	Windows 95/98/ME/NT 4.0/2000, XP	ICQ 2002 a Build#3722	Mirabilis ICQ .hpf Denial of Service	Low	CyberNotes-2002-08
Mirabilis ¹¹⁴⁷	Windows 95/98/ME/NT 4.0/2000, XP	ICQ 2002 a Build 3727, Build 3722	Mirabilis ICQ Sound Scheme Remote Configuration Modification & Predictable File Location	High	CyberNotes-2002-15
Mirabilis ¹¹⁴⁸	Windows 95/98/ME/NT 4.0/2000, XP	ICQ, 2001 b Build #3659, #3638, #3636, 2001 a, 2002 a Build #3727, #3722	ICQ 2001/2002 Remote Denial of Service	Low	CyberNotes-2002-15
MIT ¹¹⁴⁹	Unix	PGP Public Key Server 0.9.2, 0.9.4	PGP Public Key Server Remote Buffer Overflow	Medium	CyberNotes-2002-11
MIT ¹¹⁵⁰	Unix	CGIEmail 1.6	CGIEmail Mail Relay	Medium	CyberNotes-2002-13
mnoGo Search ¹¹⁵¹	Multiple	mnoGo Search 3.1.19	mnoGoSearch Buffer Overflow	High	CyberNotes-2002-10
Mobydisk ¹¹⁵²	Windows	Moby NetSuite 1.0, 1.2	Moby NetSuite POST Handler Denial of Service	Low	CyberNotes-2002-25
mod_ssl ¹¹⁵³ <i>Vendors issue patches^{1154, 1155, 1156, 1157}</i>	Multiple	mod_ssl 2.8.5-2.8.9	Mod_SSL HTAccess Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-13 CyberNotes-2002-14
Mojo Mail ¹¹⁵⁸	Unix	Mojo Mail 2.7	Mojo Mail Cross-Site Scripting	High	CyberNotes-2002-22
Mollensoft Software ¹¹⁵⁹	Windows NT	Enceladus Server Suite 2.6.1	Enceladus Server Suite Directory Traversal	Medium	CyberNotes-2002-25
Mollensoft Software ¹¹⁶⁰	Windows	Enceladus Server Suite 3.9	Mollensoft Software Enceladus Server Suite CD Buffer Overflow	High	CyberNotes-2002-25
Mondo Soft, Inc. ¹¹⁶¹	Windows	MondoSearch 4.4	MondoSearch Source Disclosure	Medium	CyberNotes-2002-21
Monkey ¹¹⁶²	Unix	Monkey HTTP Daemon 0.1.4	Monkey HTTP Server Sensitive Information	Medium	CyberNotes-2002-20
Monkey ¹¹⁶³	Unix	Monkey HTTP Daemon 0.1.4, 0.4-0.4.2, 0.5	Monkey HTTP Server Cross-Site Scripting	High	CyberNotes-2002-20
Monkey ¹¹⁶⁴	Unix	Monkey HTTP Daemon 0.4-0.4.2, 0.5	Monkey Remote Denial of Service	Low	CyberNotes-2002-23
Mosix Project ¹¹⁶⁵	Unix	ClumpOS 5.4	ClumpOS Default VNC Password	High	CyberNotes-2002-09
Mosix Project ¹¹⁶⁶	Unix	Mosix 1.5.7, OpenMosix 2.4.17	Mosix Malformed Packet Denial of Service	Low	CyberNotes-2002-09
Mozilla & Netscape ¹¹⁶⁷	Windows 95/98/ME/NT 4.0/2000, XP, MacOS 9.0/9.0.4/ 9.1/ 9.2/ 9.2.1, MacOS X 10.x, Unix	Browser 0.9.2-0.9.9, 1.0, 1.0 RC1&2, 1.0; Netscape 6.0 1, 6.0 Mac, 6.0, 6.1, 6.2-6.2.2	Mozilla JavaScript URL Host Spoofing Arbitrary Cookie Access	Medium	CyberNotes-2002-15
Mozilla Project ¹¹⁶⁸	Unix	Browser 0.8	Mozilla Predictable Temporary File Symbolic Link Attack	Medium	CyberNotes-2002-01
Mozilla Project ¹¹⁶⁹	Windows 95/98/NT 3.5.1/4.0	BugZilla 2.4, 2.6, 2.8, 2.10, 2.12, 2.14	BugZilla Multiple Vulnerabilities	Medium/High (High for the buglist. cgi script vulnerability.)	CyberNotes-2002-01

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Mozilla Project ¹¹⁷⁰	Windows 95/98/NT 3.5.1/4.0	BugZilla 2.4, 2.6, 2.8, 2.10, 2.12, 2.14	BugZilla LDAP Authentication Bypass	Medium	CyberNotes-2002-01
Mozilla Project ¹¹⁷¹	Multiple	BugZilla 2.14, 2.14.1	Multiple BugZilla Security	Medium	CyberNotes-2002-12
Mozilla Project ¹¹⁷²	Unix	Mozilla Browser 1.0, 1.0 RC1&2, 1.1 Alpha	Mozilla 'FTP View' Cross-Site Scripting	High	CyberNotes-2002-16
Mozilla Project ¹¹⁷³	Unix	Bonsai 1.3	Bonsai Multiple Cross Site Scripting & Path Disclosure Vulnerabilities	Medium/High (High if arbitrary code is executed)	CyberNotes-2002-17
Mozilla Project ¹¹⁷⁴	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/ 9.0.4/ 9.1/ 9.2/ 9.2.1/9.2.2, MacOS X 10.x, BeOS 5.0, Unix	Mozilla Browser 0.9.3-0.9.9, 1.0, 1.0.1, 1.1	Mozilla OnUnload Referer Information Leakage	Medium	CyberNotes-2002-19
Mozilla Project ¹¹⁷⁵	Multiple	BugZilla 2.14- 2.14.4, 2.16	BugZilla Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Mozilla Project ¹¹⁷⁶	Multiple	Mozilla Browser 1.0	Mozilla Multiple Vulnerabilities	Low/ Medium/High (Low if a Denial of Service, Medium if sensitive information is obtained and High if arbitrary code can be executed)	CyberNotes-2002-20
Mozilla Project ¹¹⁷⁷	Multiple	BugZilla 2.10, 2.12, 2.14, 2.14.1- 2.14.4, 2.16, 2.16.1, 2.17	BugZilla Cross-Site Scripting	High	CyberNotes-2002-24
Mozilla/ Netscape ¹¹⁷⁸	Windows 95/98/ME/NT 4.0, XP, MacOS 9.0/9.0.4, 9.1/9.2/ 9.2.1/9.2.2, MacOS X 10.x	Mozilla Browser 0.9.7, 0.9.8, 0.9.9, 1.0 RC1; Netscape 6.1-6.2.2	Mozilla / Netscape 6 XMLHttpRequest File Disclosure	Medium	CyberNotes-2002-09
Mozilla/ Netscape ¹¹⁷⁹	Windows 95/98/ME/NT 4.0/2000, XP, Mac OS 9.0, 9.0.4, 9.1, 9.2, MacOS X 10.x, Unix	Mozilla Browser 0.9.2.1, 0.9.2, 0.9.3, 0.9.4.1, 0.9.4-0.9.9, 1.0, 1.0 RC1&2; Netscape Communicator 4.0.4-4.08, 4.0, 4.5-4.7, 4.51, 4.61, 4.72-4.77, Netscape 6.0 1, 6.0 Mac, 6.0-6.2.2	Netscape / Mozilla Malformed E-mail Denial of Service	Low	CyberNotes-2002-12
Mozilla/ Netscape ¹¹⁸⁰	Multiple	Mozilla Browser 0.9.6-0.9.9, 1.0, 1.0.1, 1.1; Netscape 6.2- 6.2.3, 7.0	Netscape/ Mozilla JAR Remote Buffer Overflow	High	CyberNotes-2002-24
Mozilla/ Netscape ¹¹⁸¹	Windows 95/98/ME NT 4.0/2000, Unix	Mozilla Browser 1.0, 1.0 RC1&RC2, 1.0.1, 1.1, 1.1 Alpha & Beta, 1.2 Beta; Netscape Communicator 4.61, 4.72-4.79, 6.1, 6.2.3	Netscape/ Mozilla POP3 Mail Handler Integer Overflow	Medium	CyberNotes-2002-24
MRTG ¹¹⁸²	Windows NT 4.0/2000, Unix	Multi Router Traffic Grapher CGI 2.9.17-win32, 2.9.17-unix	MRTG CGI File Display	Medium	CyberNotes-2002-03
MRTG Configuration Generator ¹¹⁸³	Multiple	MRTG config 0.5.9	MRTG Path Disclosure Vulnerabilities	Medium	CyberNotes-2002-03
Multiple Vendors ¹¹⁸⁴	Unix	GNU GZip 1.3 -1.2.4a	GZip Long File Name Buffer Overflow	High	CyberNotes-2002-01

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ¹¹⁸⁵	Multiple	Links Links 0.96; University of Kansas Lynx 2.7, 2.8, 2.8.4; W3M W3M 0.1.3, 0.1.4, 0.1.6-0.1.10, W3M 0.2-0.2.3	Multiple Vendor SSL Certificate Validation	Medium	CyberNotes-2002-01
Multiple Vendors ¹¹⁸⁶	Unix	Linux kernel 2.2-2.2.20, 2.4-2.4.17	Linux Encrypted Loop Filesystem Replay Attack	Medium	CyberNotes-2002-01
Multiple Vendors ¹¹⁸⁷	Windows 95/98/ME/NT 4.0/2000, MacOS 9.0, Unix	AccessData SecureClean v3 build-2.0; East-Tec Eraser 2000, 5.3; Jetico BCWipe 1.07, 2.08b, 2.0, 2.13, 2.16, 2.28, 2.28.3, 2.28.4, 2.28.7, 2.33, 2.35, 2.35.1; Network Associates PGP 6.0.2, 6.5.3, 6.5.8, 7.0, 7.0.3, 7.0.4, 7.1.1, PGP Freeware 7.0.3	Multiple Vendor File Wiping Utilities	Medium	CyberNotes-2002-02
Multiple Vendors ¹¹⁸⁸	Windows 95/98/ME/NT 4.0/2000, XP	Deerfield D2Gfx 1.0.2; Working Resources Inc. BadBlue 1.5	Multiple Vendor Directory Traversal	Medium	CyberNotes-2002-02
Multiple Vendors ¹¹⁸⁹	Windows 95/98/ME/NT 4.0/2000, XP	Deerfield D2Gfx 1.0.2; Working Resources Inc. BadBlue Enterprise Edition 1.5	Multiple Vendor Upload Feature Password Protection	High	CyberNotes-2002-02
Multiple Vendors ¹¹⁹⁰	Windows 98/ME/NT 4.0/2000, XP	Microsoft IIS 4.0, 5.0; Symantec Norton Internet Security 2001	Multiple Vendor Default File Permissions	Medium	CyberNotes-2002-02
Multiple Vendors ¹¹⁹¹	Windows 95/98/ME/NT 4.0/2000, XP, MacOS 9.0-10.1.2, Unix	Mozilla Browser 0.9.2.1-0.9.6 Netscape Communicator 4.0-4.08, 4.5BETA, 4.5-4.78, 6.0 Mac, 4.77 Mac, 6.1, 6.2	Netscape/ Mozilla Null Character	Medium	CyberNotes-2002-02
Multiple Vendors ¹¹⁹²	Multiple	Palm OS 3.5h	PalmOS Remote Denial of Service	Low	CyberNotes-2002-02
Multiple Vendors ¹¹⁹³	Windows 95/98/ME/NT 4.0/2000, XP	FastTrack KaZaA 1.2-1.5; Grokster Grokster 1.3, 1.3.3; Music City Networks Morpheus 1.3, 1.3.3	Multiple Vendor Identity Spoofing	Low/ Medium (Low for the DoS)	CyberNotes-2002-04
Multiple Vendors ¹¹⁹⁴	Windows 95/98/ME/NT 4.0/2000, XP	FastTrack KaZaA 1.2-1.5; Grokster Grokster 1.3, 1.3.3; Music City Networks Morpheus 1.3, 1.3.3	FastTrack P2P Technology Denial of Service	Low	CyberNotes-2002-04
Multiple Vendors ¹¹⁹⁵ <i>HP issues patch for MPE/iX¹¹⁹⁶</i>	Windows 95/98/ME/NT 4.0/2000, Unix	<i>MPE/iX 4.0, 4.5, 5.0, 5.5, 6.0, 6.5, 7.0</i>	Multiple Vendor SNMP Trap Handling CVE Name: CAN-2002- 0012	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-04 CyberNotes-2002-13
Multiple Vendors ¹¹⁹⁷	Windows 95/98/ME/NT 4.0/2000, MacOS 8.0/ 8.1/ 8.5.8.6/9.0, Unix	Multiple Vendors (for complete list, see: http://online.securityfocus.com/bid/4131)	Multiple Vendor HTTP CONNECT TCP Tunnel	Medium	CyberNotes-2002-04
Multiple Vendors ¹¹⁹⁸	Multiple	Ascend RADIUS versions 1.16 & prior; Cistron RADIUS versions 1.6.5 & prior; Free RADIUS versions 0.3 & prior; Gnu RADIUS versions 0.95 & prior; ICRADIUS versions 0.18.1 & prior; Livingston RADIUS versions 2.1 & prior ; RADIUS (previously known as Lucent RADIUS) versions 2.1 & prior; RADIUS Client versions 0.3.1 & prior; XTRADIUS 1.1-pre1 & prior; YARD RADIUS 1.0.19 & prior	Multiple Vendor RADIUS Denial of Service and Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ¹¹⁹⁹	MacOS 7.X, 8.X, 9.X, MacOS X 10.X	Cab Company iCab Pre 2.7, 2.71; Microsoft Internet Explorer Macintosh Edition 4.5MRJ 2.2, 4.5MRJ 2.1.4, 4.5, 5.0; Netscape Netscape 4.77 Mac, 4.78 Mac; Omni Group OmniWeb 4.0.6, 4.1beta11; Opera Software Opera Web Browser 5.0 Mac	Multiple Vendor MacOS Browser Auto File Execution	High	CyberNotes-2002-05
Multiple Vendors ¹²⁰⁰	Unix	EFingerD 1.3, 1.6.1	EFingerD Buffer Overflow	High	CyberNotes-2002-05
Multiple Vendors ¹²⁰¹	Windows 95/98/ME/NT 4.0, XP; Unix	Ethereal Group Ethereal 0.9.1; Gerald Combs Ethereal 0.8.13 & prior	Ethereal Malformed SNMP Denial of Service	Low	CyberNotes-2002-05
Multiple Vendors ¹²⁰²	Unix	Net-SNMP ucd-snmp 4.1.1, 4.1.2, 4.2.1	Net-SNMP Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-05
Multiple Vendors ¹²⁰³	Unix	Linux kernel 2.4-2.4.18	Linux UDP Fingerprinting	Medium	CyberNotes-2002-06
Multiple Vendors ¹²⁰⁴	Windows 95/98/ME/NT 40/2000, XP; MacOS 9.0-9.2.2, MacOS X 10.0-10.1.2	Microsoft Internet Explorer 5.01, 5.01SP1&2, 5.5. 5.5SP1&2, 6.0; Mozilla Browser 0.8-0.9.8; Opera Software Opera Web Browser 5.02 win32, 5.10-5.12, 6.0.1win32	Multiple Vendor JavaScript Interpreter Denial Of Service	Low	CyberNotes-2002-06
Multiple Vendors ¹²⁰⁵	Unix	Linux kernel 2.2-2.2.20, 2.3, 2.3.99, 2.4- 2.4.18	Linux Kernel d_path() Path Truncation	Medium	CyberNotes-2002-07
Multiple Vendors ¹²⁰⁶	Windows 95/98/ME/NT 4.0/2000	BindView NETrc 1.0, 3.06; Funk Software Proxy 3.0, 3.06, 3.09, 3.09a	Funk Software Proxy Multiple Vulnerabilities CVE Names: CAN-2002-0064, CAN-2002-0065, CAN-2002-0066	Medium	CyberNotes-2002-08
Multiple Vendors ¹²⁰⁷	Unix	FreeBSD FreeBSD 4.4 –RELENG, 4.5 – STABLE, RELEASE; OpenBSD OpenBSD 2.0-2.3; Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	BSD exec C Library File Descriptor Closure	High	CyberNotes-2002-09
Multiple Vendors ¹²⁰⁸	Windows 95/98/ME/NT 4.0, XP, MacOS 9.x, MacOS X 10.x, Unix	Galeon Browser 1.2, 1.2.1; Mozilla Browser 0.9.9, 1.0 RC1; Netscape 6.0-6.2.2	Netscape/ Mozilla/Galeon Local File Detection	Medium	CyberNotes-2002-09
Multiple Vendors ¹²⁰⁹	Multiple	Microsoft Visual C++.Net; StackGuard 1.2, 1.2.1, 2.0.1, 0.7 -beta	Multiple Stack Protection Scheme Function Argument Overwrite	Medium	CyberNotes-2002-09
Multiple Vendors ¹²¹⁰	Windows 95/98/ME/NT 4.0/2000, XP	ATGuard Personal Firewall 3.2; Tiny Personal Firewall 1.0, 2.0, 2.0.15	Multiple Vendor Firewall Port 53 Communication	Medium	CyberNotes-2002-10
Multiple Vendors ¹²¹¹	Multiple	MyBB DevBB 1.0; The XMB Group XMB Forum 1.6 Magic Lantern	XMB Forum Magic Lantern Cross-Site Scripting	High	CyberNotes-2002-10

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ¹²¹²	Windows 98, XP, Unix	Debian Linux 2.2 sparc, powerpc, IA-32, arm, alpha, 68k; Mandrake Soft Linux Mandrake 8.0, 8.0 ppc, 8.1, 8.1 ia64, 8.2; Microsoft Windows 98, 98SE, XP Home, XP Professional; RedHat Linux 6.2 sparc, i386, alpha, Linux 7.0 sparc, i386, alpha, Linux 7.1 ia64, i386, alpha, Linux 7.2 ia64, i386, Linux 7.3 i386; SuSE Linux 6.4 ppc, i386, alpha, Linux 7.0 sparc, ppc, i386, alpha, 7.1 x86, 7.1 sparc, ppc, alpha, Linux 7.2 i386, Linux 7.3 sparc, 7.3 ppc, i386, Linux 8.0 i386	Multiple Vendor IGMP Denial of Service	Low	CyberNotes-2002-13
Multiple Vendors ¹²¹³	Windows 95/98/NT 4.0/2000, Unix	HP Application Server 8.0; jo! jo Webserver 1.0 rc1; Macro-media JRun 3.0, 3.1, 4.0; Oracle 9i Application Server 1.0.2 .2, 9.0.2; Orion Application Server 1.5.3; Pramati Server 3.0; Sybase Enterprise Application Server 4.0	Multiple Vendor WEB-INF Directory Disclosure	Medium	CyberNotes-2002-14
Multiple Vendors ¹²¹⁴	Unix	Linux kernel 2.4.1- 2.4.19 -pre6	Linux Kernel File Descriptor Denial of Service	Low	CyberNotes-2002-14
Multiple Vendors ¹²¹⁵	Unix	Mandrake Soft Linux Mandrake 7.1, 8.0, 8.0 ppc; RedHat Linux 6.2 sparc, i386, alpha, 7.0 sparc, i386, alpha, 7.1 ia64, i386, alpha; Slackware Linux 8.0	EFSTool Commandline Argument Buffer Overflow	High	CyberNotes-2002-14
Multiple Vendors ¹²¹⁶	Windows 95/98/ME/NT 4.0/2000, XP	Microsoft Foundation Class Library 7.0; Working Resources Inc. BadBlue Personal Edition 1.7.3	Microsoft Foundation Class Library ISAPI Buffer Overflow	Low	CyberNotes-2002-14
Multiple Vendors ¹²¹⁷	Unix	dump 0.4 b10-b29; FreeBSD 3.5, 3.5 -STABLE, 3.5.1, 3.5.1 -STABLE/ RELEASE, 4.0, 4.1, 4.1.1, 4.1.1 -STABLE/ RELEASE, 4.2-4.5, 4.2-4.5-STABLE/ RELEASE, 4.6, 4.6 -RELEASE, 5.0; NetBSD 1.0-1.5.2; OpenBSD 2.0-3.1	Multiple Vendor Dump File Locking Denial of Service	Low	CyberNotes-2002-15
Multiple Vendors ¹²¹⁸	Unix	FreeBSD 3.5-4.6, 5.0, 3.5 -STABLE, 3.5.1 -STABLE/ RELEASE, 4.1.1 -STABLE/ RELEASE, 4.2 - 4.5 STABLE/ RELEASE, 4.6 -RELEASE; NetBSD 1.0-1.5.2; OpenBSD 2.0-3.1; SuSE, Linux 4.2-8.0	Tip File Locking Denial of Service	Low	CyberNotes-2002-15
Multiple Vendors ¹²¹⁹	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Microsoft Internet Explorer 5.0, 5.0.1, 5.5, 5.5SP1&2, 6.0; Opera Software Opera Web Browser 6.0.1 win32, Opera Web Browser 6.0.1 Linux, Opera Web Browser 6.0.1	Multiple Vendor Web Browser JavaScript Modifier Keypress Event Subversion	Medium	CyberNotes-2002-15
Multiple Vendors ¹²²⁰	Windows 95/98/NT 4.0/2000, MacOS X 10.x, Unix	OpenSSH 2.1-2.3, 2.5-2.5.2, 2.9, 2.9p1&2, 2.9.9, 3.0, 3.0 p1, 3.0.1, 3.0.1p1, 3.0.2, 3.0.2p1, 3.1, 3.1p1, 3.2, 3.2.2p1, 3.2.3 p1, 3.3, 3.3 p1, 3.4, 3.4 p1; SSH Communications Security SSH2 2.0-2.5, 3.0, 3.0.1, SSH2 for Unix 3.1-3.1.2, SSH2 for Win32 3.1-3.1.2	Multiple SSH Client Protocol Change Default Warning	Medium	CyberNotes-2002-15
Multiple Vendors ¹²²¹	Unix	Cisco iSCSI Linux 2.1.2.1	iSCSI Insecure Configuration File	Medium	CyberNotes-2002-16

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ¹²²²	Windows 95/98/ME/NT 4.0/2000, XP, MacOS 9.0/ 9.0.4/ 9.1/ 9.2/ 9.2.1, MacOS X 10.x, Unix	Microsoft Internet Explorer 5.0, 5.0.1, 5.5, 5.5 SP1&2, 6.0; Mozilla Browser M16, M15, 0.8, 0.9.2-0.9.9, 1.0, 1.0 RC1&2, 1.1 Beta, 1.1 Alpha; Netscape Communicator 4.0, 4.5, 4.5 BETA, 4.6, 4.7, 4.51, 4.61, 4.72, 4.73, 4.74, 4.75, 4.76, 4.77, 4.78, 6.1, Netscape 6.0 1, 6.0 Mac, 6.0, 6.1, 6.2, 6.2.1, 6.2.2; Opera Software Opera Web Browser 5.0 2 win32, 5.0 Mac, 5.0 Linux, 5.1 1 win32, 5.1 0 win32, 5.12 win32, 5.12, 6.0 win32, 6.0, 6.0.1 win32, 6.0.1 Linux, 6.0.1, 6.0.2 win32, 6.0.3 win32	Multiple Browser Vendor Same Origin Policy Design Error	Medium	CyberNotes-2002-16
Multiple Vendors ¹²²³	Windows 95/98/ME/ NT 4.0/2000	AT&T WinVNC 3.3 x, 3.3.3 R9, 3.3.3 r7 & Previous; TightVNC 1.2.0-1.2.5; Tridia TridiaVNC 1.5, 1.5.1, 1.5.2, 1.5.4	Multiple Vendor VNC Products Messaging API	Medium/High (High if arbitrary code is executed)	CyberNotes-2002-17
Multiple Vendors ¹²²⁴	Multiple	Compaq Wireless LAN WL310; Proxim Orinoco Residential Gateway RG-1000	Multiple Vendor SNMP Community String CVE Name: CAN-2002-0812	Medium	CyberNotes-2002-17
Multiple Vendors ¹²²⁵	Unix	Debian Linux 3.0; SGI IRIX 6.5.15- 6.5.17	FAM Directory File Listing	Medium	CyberNotes-2002-17
Multiple Vendors ¹²²⁶	Windows 95/98/MT/ NT 4.0/2000, Unix	GNU Privacy Guard 1.0-1.0.7; IETF OpenPGP RFC 2440; Network Associates PGP 5.0 i, 5.0 Linux, PGP 5.0, 5.5.3 i for Windows, 5.5.3 i, 5.5.5, 6.0.2i, 6.0.2, 6.5 Linux, 6.5.1 i for Unix, 6.5.1i, 6.5.3i for Windows, 6.5.3, 6.5.8, 7.0, 7.0.3, 7.0.4, 7.1, 7.1.1, 7.0.3	Multiple Vendor Ciphertext Message Disclosure	Medium	CyberNotes-2002-17
Multiple Vendors ¹²²⁷	Windows NT 3.5/ 3.5.1/4.0	GFI Mail Security for Exchange/SMTP 7.2; Network Associates WebShield SMTP 4.0.5, 4.5, 4.5.44, 4.5.74.0; Roaring Penguin Software CanIt 1.2, MIME Defang 2.14, 2.20; Trend Micro InterScan VirusWall for Windows NT 3.5, 3.51, 3.52	Multiple Vendor Email Message Fragmentation SMTP Filter Bypass CVE Name: CAN-2002-1121	High	CyberNotes-2002-19
Multiple Vendors ¹²²⁸	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/9.0.4/ 9.1/9.2/9.2.1 MacOS X 10.x, Unix, BeOS 5.0	Mozilla Browser 0.9.5-0.9.9, 1.0; Netscape 6.2-6.2.3; Opera Software Opera Web Browser 5.12. 6.0, 6.0.1	Multiple Vendor Zero Width GIF Image Files	Low/High (High if arbitrary code is executed)	CyberNotes-2002-19
Multiple Vendors ¹²²⁹	Multiple	Aladdin Systems Inc. Stuffit Expander 6.5.2; Lotus Notes Client R6, R5, 4.5 & prior, 5.0-5.0.5, 5.0.9a, 5.10, 5.11; Windows 98 With Plus! Pack, ME, XP Home, SP1, XP Professional, SP1; Verity Inc. KeyView Viewing SDK; WinZip WinZip 7.0	Multiple Vendor ZIP Files Long Filename Buffer Overflow CVE Name: CAN-2002-0370	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20
Multiple Vendors ¹²³⁰	Unix	Apache Software Foundation Tomcat 3.2-3.2.4; HP Virtual Vault 4.5, 4.6	Tomcat Directory Disclosure	Medium	CyberNotes-2002-20

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ¹²³¹	Unix	Compaq Tru64 4.0 g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f, 5.0 a PK3 (BL17), 5.0a, 5.1 a PK3 (BL3), 5.1a, 5.1 PK5 (BL19), 5.1; Hewlett Packard Systems HP-UX 10.20, 11.0, 11.11, 11.22	Multiple Vendors ypserv File Disclosure	Medium	CyberNotes-2002-21
Multiple Vendors ¹²³²	Windows 98/98/ME/ NT 4.0/2000, XP	Internet Security Systems BlackIce Defender 2.9 cap, BlackIce Server Protection 3.5 cdf; Symantec Norton Personal Firewall 2002	Multiple Vendor Firewall Auto Block Remote Denial of Service	Low/High (High if DoS best practices not in place)	CyberNotes-2002-21
Multiple Vendors ¹²³³	Unix	Apache Software Foundation Apache 2.0, 2.0.35- 2.0.42; HP HP-UX 11.0, 11.11, 11.20, 11.22	Apache 2 WebDAV CGI Information Disclosure CVE Name: CAN-2002-1156	Medium	CyberNotes-2002-22
Multiple Vendors ¹²³⁴	Unix	Apple MacOS X 10.2 (Jaguar), MacOS X Server 10.2; FreeBSD FreeBSD 4.6, 4.6 -STABLE, RELEASE; FreeS/ WAN FreeS/ WAN 1.9-1.9.6; Global Technology Associates GNAT Box Firmware 3.1-3.3; NEC BlueFire IX1035, NEC IX1010, IX1011, IX1020, IX1050, IX2010; NetBSD NetBSD 1.5, 1.5 x86, sh3, 1.5.1-1.5.3, 1.6 beta	Multiple Vendor IPsec Implementation Denial of Service CVE Name: CAN-2002-0666	Low	CyberNotes-2002-22
Multiple Vendors ¹²³⁵	Multiple	NetScreen ScreenOS 2.7.1, 2.7.1 r1-r3, 2.10 r3&r4, 3.0.1 r1&r2, 3.0.3 r1.1	Multiple Firewall Vendor Packet Flood State Table Filling Remote Denial of Service	Low/High (High if DDoS best practices not in place)	CyberNotes-2002-22
Multiple Vendors ¹²³⁶	Multiple	D-Link DI-804 4.68, DI-704 V2.56b6, V2.56b5; Linksys BEFW11S4 1.4.2 .7, EtherFast BEFW11S4 Wireless AP + Cable/DSL Router 1.37.2 b, 1.37.2, 1.37.9 b, 1.40.3, 1.42.7, WAP11 1.3, WAP11 1.4	Multiple Vendor Embedded HTTP Server Denial of Service	Low	CyberNotes-2002-23
Multiple Vendors ¹²³⁷	Unix	Linux kernel 2.4.1- 2.4.18	Linux Kernel 2.4 System Call TF Flag Denial of Service	Low	CyberNotes-2002-23
Multiple Vendors ¹²³⁸ <i>More advisories released^{1239, 1240, 1241}</i>	Unix	Solaris 2.5.1, 2.5.1_x86, _ppc, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86 Update 2; XFree86 X11R6 3.3, 3.3.2-3.3.5; HP-UX 10.10, 10.20, 10.24, 11.04, 11.0, 11.11, 11.22; SGI IRIX 6.5, 6.5.1- 6.5.13	Multiple Vendor fs.auto Remote Buffer Overrun CVE Name: CAN-2002-1317	High	CyberNotes-2002-24 CyberNotes-2002-25
Multiple Vendors ¹²⁴²	Unix	OpenBSD OpenBSD 3.0; Sun Solaris 2.6, 2.6_x86, 7.0, 7.0_x86	Multiple Vendor FTP Client Side File Overwriting CVE Name: CAN-2002-1345	Medium	CyberNotes-2002-25

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
<p>Multiple Vendors^{1243,1244}</p> <p><i>More patches released^{1245, 1246, 1247, 1248, 1249}</i></p> <p><i>Proof of Concept exploit has been published.¹²⁵⁰</i></p> <p><i>HP releases bulletin¹²⁵¹</i></p> <p><i>More patches released^{1252, 1253, 1254, 1255, 1256}</i></p> <p><i>SCO releases patch¹²⁵⁷</i></p>	Windows NT 4.0/2000, Unix	Apache Software Foundation Apache 1.3.20, 1.3.22- 1.3.26; Oracle Internet Application Server 1.0.2.1, 1.0.2.0, 8i Enterprise Edition 8.1.7.1.0, 8.1.7.0.0, 9i Application Server, 1.0.2.2, 1.0.2.1s, 1.0.2, 9.0.2, 9.0.2 release 2, 9iAS Reports 9.0.2 .1, Oracle8 8.1.7, 8.1.7.1, 8.1.7, Oracle9i Release 2 9.2 .2, 9.0.2	<p>Apache Web Server Multiple Vulnerabilities</p> <p>CVE Names: CAN-2002-0839, CAN-2002-0840, CAN-2002-0843</p>	<p>Low/High</p> <p>(High if arbitrary code can be executed)</p>	<p>CyberNotes-2002-20</p> <p>CyberNotes-2002-21</p> <p>CyberNotes-2002-22</p> <p>CyberNotes-2002-23</p> <p>CyberNotes-2002-25</p>
<p>Multiple Vendors^{1258, 1259}</p> <p><i>More vendors release upgrades¹²⁶⁰</i></p>	Unix	Hewlett Packard Secure OS software for Linux 1.0; RedHat Linux 6.2, 6.2 sparc, i386, alpha, 7.0, 7.0 i386, alpha, 7.1, 7.1 ia64, i386, alpha, 7.2, 7.2 ia64, i386, 7.3, 7.3 i386, 8.0, 8.0 i386	<p>dvips Arbitrary Command Execution</p> <p>CVE Name: CAN-2002-0836</p>	High	<p>CyberNotes-2002-21</p> <p>CyberNotes-2002-25</p>
Multiple Vendors ^{1261, 1262, 1263}	Unix	National Science Foundation Squid Web Proxy 2.0-2.4 STABLE 1&2	Squid Multiple Denial of Service Vulnerabilities	Low	CyberNotes-2002-05
<p>Multiple Vendors^{1264, 1265, 1266, 1267, 1268, 1269}</p> <p><i>RedHat releases patch¹²⁷⁰</i></p>	Unix	KTH eBones 1.2, Heimdal 0.3 e, 0.4 a-0.4 e, 0.5, 0.21; MIT Kerberos 4 1.0, 1.1, 4.0, Kerberos 5 1.0, 1.0.6, 1.1, 1.1.1, 1.2-1.2.6; NetBSD NetBSD 1.5-1.5.3, 1.6; OpenBSD OpenBSD 3.0, 3.1	<p>Multiple Vendor kadmind Remote Buffer Overflow</p> <p>CVE Name: CAN-2002-1235</p>	High	<p>CyberNotes-2002-22</p> <p>CyberNotes-2002-23</p>
<p>Multiple Vendors^{1271, 1272, 1273, 1274}</p> <p><i>Conectiva releases patch¹²⁷⁵</i></p>	Unix	Debian Linux 2.2, 2.2 sparc, powerpc, IA-32, alpha, arm, 68k, 3.0, 3.0 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, happa, arm, alpha; HP Secure OS software for Linux 1.0; RedHat 6.2, 6.2 sparc, i386, alpha, 7.0, 7.0 i386, alpha, 7.1, 7.1 ia64, i386, 7.2, 7.2 ia64, 7.3, 7.3 i386	<p>Ypserv Remote Network Information Leakage</p> <p>CVE Name: CAN-2002-1232</p>	Medium	<p>CyberNotes-2002-22</p> <p>CyberNotes-2002-23</p>
<p>Multiple Vendors^{1276, 1277, 1278, 1279, 1280}</p> <p><i>Conectiva releases advisory¹²⁸¹</i></p>	Unix	EnGarde Secure Linux 1.0.1; Mandrake Soft Linux Mandrake 7.2, 8.0, 8.0 ppc, 8.1, 8.1 ia64, 8.2, 8.2 ppc, 9.0, Single Network Firewall 7.2; mod_ssl, 2.4.10, 2.8.9; OpenPKG OpenPKG Current, 1.0, 1.1	<p>Mod_SSL Cross-Site Scripting</p> <p>CVE Name: CAN-2002-1157</p>	High	<p>CyberNotes-2002-22</p> <p>CyberNotes-2002-23</p>
Multiple Vendors ^{1282, 1283}	Unix	FreeBSD 2.0-4.4; NetBSD 1.3-1.5.2; OpenBSD 2.0-3.0	BSD exec() Race Condition	Medium	CyberNotes-2002-02
Multiple Vendors ^{1284, 1285}	Unix	Easy Software Products CUPS 1.0.4, 1.1.7, 1.1.10, 1.1.13	Multiple Vendor CUPS Buffer Overflow	High	CyberNotes-2002-04
Multiple Vendors ^{1286, 1287}	Unix	Linux kernel 2.4.9, 2.4.14- 2.4.17, 2.4.18pre-1- 2.4.18pre-7	Linux Kernel IRC DCC Arbitrary Connection Access	Medium	CyberNotes-2002-05
			CVE Name: CAN-2002-0060		

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ^{1288, 1289}	Unix	HP Java JRE /JDK HP-UX 1.1.8, 1.2.2, 1.3; Sun JDK (Solaris Production Release) 1.1.8_14, 1.1.8_008, JDK (Windows Production Release) 1.1.8_008, JRE (Linux Production Release) 1.2.2_010, 1.3_05, (Solaris Production Release) 1.1.8_14, 1.2.2_10, 1.3_05, 1.3.1_01, 1.1.8_008, 1.2.2_10, (Windows Production Release) 1.1.8_008, 1.2.2_010, 1.3_05, 1.3.1_01a, SDK (Linux Production Release) 1.2.2_010, 1.3_05, 1.3.1_01, (Solaris Production Release) 1.2.2_10, 1.3_05, 1.3.1_01, 1.2.2_010, (Windows Production Release) 1.2.2_10, 1.3_05, 1.3.1_01a	Multiple Vendor Java Virtual Machine Bytecode Verifier CVE Name: CAN-2002-0076	High	CyberNotes-2002-06
Multiple Vendors ^{1290, 1291}	Unix	HP Java Web Start 1.0.00, 1.0.1.00; Sun Java Web Start 1.0, 1.0.1_01, 1.0.1	Multiple Vendor Java Web Start Unsigned Application	Medium	CyberNotes-2002-06
Multiple Vendors ^{1292, 1293}	Unix	Compaq Tru64 4.0 g, 4.0 f, 5.0 a, 5.1 a, 5.1; HP-UX 10.10, 10.20, 10.24, 11.0 4, 11.0, 11.11; IBM AIX 4.3-4.3.3; Sun Solaris2.4, 2.4_x86, 2.5, 2.5_x86, 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	CDE DTPrintInfo Buffer Overflow	High	CyberNotes-2002-09
Multiple Vendors ^{1294, 1295}	Unix	Linux kernel 2.4.4-2.4.18, kernel 2.4.19 -pre1-pre6	Linux NetFilter NAT Information Leakage	Medium	CyberNotes-2002-10
Multiple Vendors ^{1296, 1297}	Unix	FreeBSD 4.0-4.6, 4.1.1-STABLE-4.5 -STABLE, 4.1.1-RELEASE-4.6-RELEASE; OpenBSD 3.0, 3.1	Multiple Vendor KTrace SUID/SGID Process Tracing	Medium	CyberNotes-2002-14
Multiple Vendors ^{1298, 1299}	Unix	diet libc 0.18; GNU gcc 2.7.2, 2.95, 3.0.3.1.1, glibc 2.0-2.0.6, 2.1-2.1.3, 2.1.9 & greater, 2.2-2.2.5, 2.3.10, glibc2 2.3.10, GNAT 3.14b	Multiple Vendor calloc() Integer Overflow	High	CyberNotes-2002-16
Multiple Vendors ^{1300, 1301}	Unix	FreeBSD 4.0-4.6, 4.1.1-4.6 STABLE, 4.1.1 - 4.3 RELEASE, 4.3 - 4.4 RELENG, 4.5 - 4.6 RELEASE; NetBSD 1.4.1-1.4.3, 1.5-1.5.3, 1.6 beta; OpenBSD 3.0, 3.1	Multiple Vendor BSD pppd Arbitrary File Permission Modification	Medium	CyberNotes-2002-16
Multiple Vendors ^{1302, 1303}	Unix	Caldera OpenUnix 8.0, UnixWare 7, 7.1.0, 7.1.1; Compaq Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1; HP HP-UX 10.10, 10.20, 10.24, 11.0, 11.11; IBM AIX 4.3.3, 5.1; Sun Solaris 2.5.1, 2.6, 7.0, 8.0, 9.0; Xi Graphics DeXtop 2.1	Multiple Vendor CDE ToolTalk Database Server Buffer Overflow CVE Name: CAN-2002-0679	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-17
Multiple Vendors ^{1304, 1305}	Unix	Linux kernel 2.2.1- 2.2.21	Multiple Linux Kernel 2.2 Security	Medium/High (High if root privileges can be obtained)	CyberNotes-2002-21
Multiple Vendors ^{1306, 1307}	Unix	Linux kernel 2.4.1- 2.4.18	Linux Kernel Multiple Vulnerabilities	Low/ Medium (Medium if elevated privileges can be obtained)	CyberNotes-2002-21
Multiple Vendors ^{1308, 1309}	Unix	Linux-HA heartbeat 9.4.9.1, 0.4.9a -0.4.9c, 0.9.4 d	Linux-HA Heartbeat Remote Buffer Overflow	High	CyberNotes-2002-21

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ^{1310, 1311}	Mac OS X 10.X, Unix	Apple MacOS X 10.0-10.0.4, 10.1--10.1.5, 10.2 (Jaguar), 10.2.1, MacOS X Server 10.0, 10.2-10.2.1; GNU glibc 2.0-2.0.6, 2.1, 2.1.1-6, 2.1.1- 2.1.3, 2.1.3-10, 2.2-2.2.5, 2.3, 2.3.1; SGI IRIX 6.5-6.5.13, 6.5.14 m- 6.5.17 m, 6.5.14 f- 6.5.14 m	Multiple Vendor Sun RPC LibC Remote Denial of Service CVE Name: CAN-2002-1265	Low	CyberNotes-2002-23
Multiple Vendors ^{1312, 1313}	Unix	Astaro Security Linux 2.0 16, 23-27, 30, Linux 3.2 00, 10, 11; ISC BIND 4.9.2- 4.9.10	ISC BIND DNS Resolver Buffer Overflow CVE Name: CAN-2002-0029	High	CyberNotes-2002-24
Multiple Vendors ^{1314, 1315, 1316} <i>SCO releases patch¹³¹⁷</i>	Unix	HP Secure OS software for Linux 1.0; Mandrake Soft Corporate Server 1.0.1, Mandrake 7.0, 7.1, 7.2, 8.0, 8.0 ppc, 8.1, 8.1 ia64, 8.2, Single Network Firewall 7.2; RedHat Linux 6.0, 6.0 sparc, alpha, 6.1, 6.1 sparc, alpha, 6.2, 6.2 sparc, alpha, 7.0, 7.0 alpha, 7.1, 7.1 ia64, alpha, 7.2, 7.2 ia64, alpha, 7.3; Sun Cobalt RaQ-RaQ 5, RaQ XTR, Cache RaQ series, Qube-Qube3, Control Station	Util-linux File Locking Race Condition CVE Name: CAN-2002-0638	Medium	CyberNotes-2002-16 CyberNotes-2002-22
Multiple Vendors ^{1318, 1319, 1320}	Unix	FreeBSD 4.3, 4.3 -STABLE, 4.3 -RELENG, 4.3 -RELEASE 4.4, 4.4 -STABLE, 4.4 -RELENG, 4.5, 4.5 -STABLE, 4.5 -RELEASE, 4.6, 4.6 -RELEASE; ISC BIND 4.9, 4.9.3-4.9.7, 8.1, 8.1.1, 8.1.2, 8.2, 8.2.1-8.2.3; NetBSD NetBSD 1.4, 1.4 x86, SPARC, arm32, ALPHA, 1.4.1, 1.4.1 x86, SPARC, sh3, arm32, ALPHA, 1.4.2, 1.4.2 x86, SPARC, arm32, ALPHA, 1.4.3, 1.5, 1.5 x86, sh3, 1.5.1, 1.5.2; OpenBSD OpenBSD 2.7-3.1	Multiple Vendor libc DNS Resolver Code Buffer Overflow	High	CyberNotes-2002-13
Multiple Vendors ^{1321, 1322, 1323}	Unix	Solaris 2.5.1 2.6 7.0, 8.0, 9.0; HP-UX 10.10 10.20 11.00 11.11; Compaq Tru64 4.0f, 4.0g, 5.0a, 5.1, 5.1a; Xi Graphics deXtop CDE 2.1; IBM AIX 4.3.3, 5.1.0; Caldera OpenUnix, 8.0, UnixWare 7.1.1; SGI IRIX 5.2, 5.3, 6.0, 6.0.1, 6.1-6.5.16	Multiple CDE ToolTalk Vulnerabilities CVE Names: CAN-2002-0677, CAN-2002-0678	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-14
Multiple Vendors ^{1324, 1325, 1326}	Unix	PERL-MailTools 1.13, 1.15, 1.40, 1.42, 1.44, 1.47, 1.1401	PERL-MailTools Remote Command Execution	High	CyberNotes-2002-23
Multiple Vendors ^{1327, 1328, 1329, 1330}	Unix	AT 3.1.7, 3.1.8	AT Command line Execution CVE Name: CAN-2002-0004	High	CyberNotes-2002-02
Multiple Vendors ^{1331, 1332, 1333}	Unix	Apache-SSL Apache-SSL 1.40-1.46, mod_ssl, mod_ssl 2.7.1-2.8.6	Apache Mod_SSL/ Apache-SSL Buffer Overflow	High	CyberNotes-2002-05
Multiple Vendors ^{1334, 1335, 1336, 1337}	Unix	OSSP mm 1.0.0- 1.0.12, 1.1.0-1.1.3	MM Shared Memory Library Temporary File Privilege Escalation CVE Name: CAN-2002-0658	Medium	CyberNotes-2002-16

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ^{1338, 1339, 1340, 1341}	Unix	Compaq Tru64 4.0 g PK3 (BL17), 4.0g, 4.0 f PK7 (BL18), 4.0f, 5.0 a PK3 (BL17), 5.0a, 5.1 a PK3 (BL3), 5.1a, 5.1 PK5 (BL19), 5.1; HP HP-UX 10.20, 11.0, 11.11, 11.22; Caldera OpenLinux 2.2-2.4; SCO OpenServer 5.0.5, 5.0.6; Sun Micro-systems, Inc. Solaris 2.6, 7, 8, and 9; IBM AIX 4.3.3, 5.0.1	Multiple Platforms ypxfrd Information Disclosure	Medium	CyberNotes-2002-21
Multiple Vendors ^{1342, 1343, 1344, 1345,}	Unix	FreeBSD 4.5, 4.6; GNU glibc 2.0-2.0.6, 2.1-2.1.3, 2.2-2.2.5	Multiple Vendor libc DNS Resolver Information Leakage CVE Name: CAN-2002-1146	Medium	CyberNotes-2002-23
Multiple Vendors ^{1346, 1347, 1348, 1349, 1350, 1351}	Unix	GNU glibc 2.0-2.2.4	Glibc File Globbing Heap Corruption CVE Name: CAN-2001-0886	High	CyberNotes-2002-01
Multiple Vendors ^{1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359}	Unix	rsync 2.3.1, 2.3.2-1.2 sparc & PPC, 2.3.2-1.2 m68k, intel, ARM & alpha, 2.3.2, 2.4.1, 2.4.3, 2.4.4, 2.4.6	rsync Signed Variable CVE Name: CAN-2002-0048	High	CyberNotes-2002-03
Multiple Vendors ^{1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368,}	Unix	ZLib 1.0-1.0.9, 1.1-1.1.3	ZLib Compression Library CVE Name: CAN-2002-0059	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-06
Multiple Vendors ^{1369, 1370, 1371, 1372, 1373, 1374, 1375}	Unix	PHP 3.0.10- 3.0.18, 4.0.1-4.0.7, 4.1.0, 4.1.1	PHP POST Request Buffer Overflows	High	CyberNotes-2002-05
Multiple Vendors ^{1376, 1377, 1378, 1379, 1380, 1381, 1382}	Unix	Todd Miller Sudo 1.5.9, 1.6-1.6.2, 1.6.3 p1- 1.6.3 p7, 1.6.3, 1.6.4 p1-1.6.4 p2, 1.6.4, 1.6.5 p1-1.6.5 p2, 1.6.5	Sudo Password Prompt Heap Overflow CVE Name: CAN-2002-0184	High	CyberNotes-2002-09
Multiple Vendors ^{1383, 1384, 1385, 1386, 1387, 1388, 1389, 1390}	Unix	OpenSSH 2.1-2.3, 2.5-2.5.2, 2.9p2, 2.9p1, 2.9, 2.9.9-3.0.2	OpenSSH Channel Code Off-By-One CVE Name: CAN-2002-0083	High	CyberNotes-2002-05
Multiple Vendors ^{1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398}	MacOS X 10.x, Unix	Apple MacOS X 10.0- 10.0.4, 10.1-10.1.5; FreeBSD 4.0-4.6, 4.1.1-4.6 STABLE, 4.1.1- 4.3 RELEASE, 4.3 - 4.4 RELENG, 4.5-4.6 - RELEASE; MIT Kerberos 5 1.0, 1.0.6, 1.1- 1.2.5; NetBSD 1.4-1.4.3, 1.5-1.5.3, 1.6; OpenBSD 2.0-3.1; Sun 2.5.1, 2.5.1_x86, _ppc, 2.6, 2.6_x86, 2.7, 2.7 sparc, 2.8, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0; OpenAFS 1.0-1.0.4, 1.1-1.2.5, 1.3-1.3.2	Multiple Vendor Sun RPC xdr_array Buffer Overflow	High	CyberNotes-2002-16
Multiple Vendors ^{1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1407} <i>More vendors issue updates^{1408, 1409, 1410}</i>	Windows 95/98/NT 4.0/2000, XP, MacOS X 10.0- 10.0.3, Unix	Apache Software Foundation Apache 1.0-1.0.3, 1.0.5, 1.1, 1.1.1, 1.2, 1.2.5, 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.9, 1.3.11- 1.3.14, 1.3.11 win32-1.3.20 win32, 1.3.14 Mac, 1.3.17-1.3.20, 1.3.22- 1.3.24, 1.3.22 win32- 1.3.24 win32, 2.0. 2.0.28, 2.0.32, 2.0.35, 2.0.36	Multiple Vendor Apache Chunked-Encoding Memory Corruption CVE Name: CAN-2002-0392	Low/High (High if arbitrary code can be executed or if root access is obtained)	CyberNotes-2002-13 CyberNotes-2002-14

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ^{1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1419, 1420} <i>Vendors' updates issued and exploit scripts published.</i> ^{1421, 1422, 1423, 1424, 1425, 1426}	Unix	HP HP-UX Secure Shell A.03.10; OpenSSH 1.2.2, 1.2.3, 2.1, 2.1.1, 2.3, 2.5, 2.5.1, 2.5.2, 2.9, 2.9 p1&2, 2.9.9, 3.0, 3.0 p1, 3.0.1, 3.0.1 p1, 3.0.2, 3.0.2 p1, 3.1, 3.1 p1, 3.2, 3.2.2 p1, 3.2.3 p1, 3.3, 3.3 p1	OpenSSH 'BSD_AUTH' or 'SKEY' Authentication	High	CyberNotes-2002-13 CyberNotes-2002-14
Mustata Bogdan, ¹⁴²⁷	Multiple	Zero HTTP Server 1.5	Zero HTTP Server Directory Traversal	Medium	CyberNotes-2002-25
Mutt Development Team ^{1428, 1429, 1430, 1431, 1432, 1433, 1434,}	Unix	Mutt 0.93.2, 1.0.1, 1.2.5, 1.3.12, 1.3.16, 1.3.17, 1.3.22, 1.3.24	Mutt Address Handling Buffer Overflow	High	CyberNotes-2002-01
My Postcards ¹⁴³⁵	Unix	My Postcards Platinum 5.0, 6.0	MagicCard. 'magiccard.cgi' Sensitive Information	Medium	CyberNotes-2002-13
MyBB ¹⁴³⁶	Multiple	DevBB 1.0	DevBB install.php Administrative Access	High	CyberNotes-2002-10
MyMarket ¹⁴³⁷	Unix	MyMarket 1.71	MyMarket Cross-Site Scripting	High	CyberNotes-2002-22
myPHP Nuke ¹⁴³⁸	Multiple	myPHP Nuke 1.8.8	myPHPNuke File Disclosure	Medium	CyberNotes-2002-21
myServer ¹⁴³⁹	Windows NT	myServer 0.2, 0.11	myServer Directory Traversal	Medium	CyberNotes-2002-25
MySimpleNews ¹⁴⁴⁰	Unix	MySimpleNews 1.0	MySimpleNews Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-20
MySQL AB ¹⁴⁴¹	Windows	MySQL 3.20.32 a, 3.22.26-3.22.30, 3.22.32, 3.23.2- 3.23.5, 3.23.8- 3.23.10, 3.23.23- 3.23.31, 3.23.34, 3.23.36- 3.23.52	MySQL Multiple Vulnerabilities	Medium	CyberNotes-2002-17
MySQL AB ¹⁴⁴²	Windows NT	MySQL 3.23.49, 4.0.0, 4.0.1	MySQL Buffer Overflow	High	CyberNotes-2002-20
MyWeb Server ¹⁴⁴³	Windows 95/98/ME/NT 4.0/2000	MyWeb Server 1.0.1, 1.0.2	MyWeb Server GET Request Buffer Overflow	High	CyberNotes-2002-14
MyWeb Server ¹⁴⁴⁴	Windows 95/98/ME/ NT 4.0/2000	MyWeb Server 1.0.2	MyWeb Server Multiple Vulnerabilities	Low/ Medium/High (Medium if sensitive information is obtained and High if arbitrary code is executed)	CyberNotes-2002-17
MyWeb Server ¹⁴⁴⁵	Windows 95/98/ME/ NT 4.0/2000	MyWeb Server 1.0.0-1.0.2	My Web Server Remote Denial of Service	Low	CyberNotes-2002-21
Namazu Project ¹⁴⁴⁶	Unix	Namazu 2.0.7, 2.0.8	Namazu Search System Cross-Site Scripting	High	CyberNotes-2002-01
National Instruments ¹⁴⁴⁷	Windows 98/2000, Unix	LabVIEW 5.1.1, 6.0, 6.1	LabVIEW HTTP Request Denial of Service	Low	CyberNotes-2002-09
National Science Foundation ¹⁴⁴⁸	Unix	Squid Web Proxy 2.0, 2.1, 2.2 STABLE5, 2.2, 2.3 STABLE 2-5, 2.3, 2.3.1, 2.4, 2.4 STABLE 1-4, 2.4 STABLE 6	Squid Compressed DNS Denial of Service	Low	CyberNotes-2002-07
National Science Foundation ^{1449, 1450, 1451, 1452}	Unix	Squid-2.x up to and including 2.4. STABLE6	Squid Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-14
National Science Foundation ^{1453, 1454, 1455, 1456, 1457}	Unix	Squid Web Proxy 2.0- 2.4	Squid Web Proxy Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
nCipher ¹⁴⁵⁸	Windows 2000	MSCAPI CSP 5.50	MSCAPI CSP Install Wizard Incorrect Key Generation	Medium	CyberNotes-2002-10
nCipher ¹⁴⁵⁹	Multiple	nForce. nShield	nCipher Message Signature Verification	Medium	CyberNotes-2002-17
NCipher Corporation ¹⁴⁶⁰	Windows NT 4.0/2000	NForce, nShield	ConsoleCall Back Class With JRE 1.4.0 Smart Card Passphrase Leak	Medium	CyberNotes-2002-13
NEC ¹⁴⁶¹	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Socks4 4.2, 4.2.1, 4.2.2, 4.3 .beta2, 4.3 .beta.pl	Socks4 User Name Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-14
NEC ¹⁴⁶²	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Socks5 1.0 r5-1.0 r10	Socks5 User Name Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-14
NEC ¹⁴⁶³	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Socks5 1.0r5- 1.0r11	Socks5 Off-By-One Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-14
NeoSoft Corp. ¹⁴⁶⁴	Windows	NeoBook 4.0	NeoBook 4 ActiveX Control	High	CyberNotes-2002-24
NetBSD ¹⁴⁶⁵	Unix	NetBSD 1.0-1.5.2	Multiple Vendor TalkD User Validation	Medium	CyberNotes-2002-07
NetBSD ¹⁴⁶⁶	Unix	NetBSD 1.4, 1.4 x86, SPARC, arm32, Alpha, 1.4.1, 1.4.1 x86, 1 SPARC, sh3, arm32, Alpha, 1.4.2, 1.4.2 x86, SPARC, arm32, Alpha, 1.4.3, 1.5, 1.5 x86, sh3, 1.5.1-1.5.3, 1.6 beta	NetBSD Repeated TIOSTTY IOCTL Buffer Overflow	Low	CyberNotes-2002-19
NetBSD ¹⁴⁶⁷	Unix	NetBSD 1.4, 1.4 x86, SPARC, arm32, Alpha, 1.4.1, 1.4.1 x86, 1 SPARC, sh3, arm32, Alpha, 1.4.2, 1.4.2 x86, SPARC, arm32, Alpha, 1.4.3, 1.5, 1.5 x86, sh3, 1.5.1-1.5.3	NetBSD LibC SetLocale Buffer Overflow	High	CyberNotes-2002-19
NetBSD ¹⁴⁶⁸	Unix	NetBSD 1.4, 1.4 x86, SPARC, arm32, Alpha, 1.4.1, 1.4.1 x86, 1 SPARC, sh3, arm32, Alpha, 1.4.2, 1.4.2 x86, SPARC, arm32, Alpha, 1.4.3, 1.5, 1.5 x86, sh3, 1.5.1-1.5.3	NetBSD IPv4 Multicast Tools Buffer Overflow	High	CyberNotes-2002-19
NetBSD ¹⁴⁶⁹	Unix	NetBSD 1.5-1.5.3, 1.6	NetBSD talkd Buffer Overflow	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-21
NetBSD ¹⁴⁷⁰	Unix	NetBSD 1.5-1.5.3, 1.6	NetBSD Trek Buffer Overflow	Medium	CyberNotes-2002-22
NetBSD ¹⁴⁷¹	Unix	NetBSD 1.5-1.5.3, 1.6	NetBSD ftpd Firewall State Table Corruption	Medium	CyberNotes-2002-24
Netfilter. org ¹⁴⁷²	Unix	Linux kernel 2.4, 2.4.1- 2.4.19, 2.5.0- 2.5.31	Linux Netfilter/ IPTables IP Queuing Arbitrary Network Traffic Reading	Medium	CyberNotes-2002-25
Netgear ¹⁴⁷³	Multiple	RP114 Cable/DSL Web Safe Router Firmware 3.26	RP114 Cable/DSL Web Safe Router Denial of Service	Low	CyberNotes-2002-02
Netgear ¹⁴⁷⁴	Multiple	RT314/RT311 Gateway Router Firmware 3.22, 3.24, 3.25	RT314/RT311 Gateway Router Cross-Site Scripting	High	CyberNotes-2002-03
Netgear ¹⁴⁷⁵	Multiple	Netgear RM-356, RT-338	Netgear Denial Of Service	Low	CyberNotes-2002-04
NetGear ¹⁴⁷⁶	Multiple	FM114P	NetGear FM114P Prosafe URL Filter Bypassing	Medium	CyberNotes-2002-19
NetGear ¹⁴⁷⁷	Multiple	FVS318 1.1	FVS318 Username/ Password Disclosure	Medium	CyberNotes-2002-20

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Netgear ¹⁴⁷⁸	Multiple	FM114P Wireless Firewall	FM114P Wireless Firewall Remote Denial of Service	Low/High (High if DoS best practices not in place)	CyberNotes-2002-21
Netgear ¹⁴⁷⁹	Multiple	FM114P Wireless Firewall	FM114P Wireless Firewall Plaintext Password	Medium	CyberNotes-2002-21
NetGear ¹⁴⁸⁰	Multiple	RP114 Cable/DSL Web Safe Router Firmware 3.26	RP114 Administrative Access Via External Interface	High	CyberNotes-2002-13
Netopia ¹⁴⁸¹	MacOS	Timbuktu Pro for Macintosh 6.0.1	Timbuktu Pro Denial of Service	Low	CyberNotes-2002-02
Netris ¹⁴⁸²	Unix	Netris 0.3-0.5	Netris Remote Denial of Service	Low	CyberNotes-2002-19
Netscape ¹⁴⁸³	Multiple	Netscape Enterprise Server for NetWare 4/5 5.0	Netscape Enterprise Web Server for NetWare Information Disclosure	Medium	CyberNotes-2002-11
Netscape ¹⁴⁸⁴	Windows 95/98/NT 4.0/2000, Unix	Communicator 4.77	Netscape Composer Buffer Overflow	High	CyberNotes-2002-12
Netscape ¹⁴⁸⁵	Multiple	Communicator 4.0, 4.5- 4.7, 4.51, 4.61, 4.72- 4.79	Netscape Java Virtual Machine Insecure Cal	High	CyberNotes-2002-24
Netscape ¹⁴⁸⁶	Windows 95/98/ME/ NT 4.0/2000, Unix	Communicator 4.6, 4.61, 4.7, 4.72-4.78	Netscape Predictable Directory Structure CVE Name: CAN-2002-1204	Medium	CyberNotes-2002-24
Netscape ¹⁴⁸⁷	Windows 95/98/ME/ NT 4.0/2000	Netscape Communicator 4., 4.5, 4.51, 4.6, 4.61, 4.7, 4.72-4.79	Netscape Java canConvert() Buffer Overflow	High	CyberNotes-2002-24
Netscape iPlanet ¹⁴⁸⁸	Windows NT 4.0/2000, Unix	Enterprise Server 3.0-3.6, Edition 4.0, 4.1; iPlanet E-Commerce Solutions iPlanet Web Server 6.0, Enterprise Edition 4.0-4.1	Netscape Enterprise Denial of Service	Low	CyberNotes-2002-01
Netscape iPlanet ¹⁴⁸⁹	Windows NT 4.0/2000, Unix	Enterprise Server 3.0-3.6, Edition 4.0, 4.1; iPlanet E-Commerce Solutions iPlanet Web Server 6.0, Enterprise Edition 4.0-4.1	Netscape Enterprise Web Server Brute Force Authentication Attacks	Medium	CyberNotes-2002-01
Netscape/Mozilla ¹⁴⁹⁰	Windows 95/98/NT 4.0, Unix	Mozilla Browser 0.9.9, 1.0 RC1; Netscape Communicator 6.0, 6.0.1, 6.1	Netscape/ Mozilla IRC Buffer Overflow	Low	CyberNotes-2002-09
NetScreen ¹⁴⁹¹	Multiple	ScreenOS 3.0.0, 3.0.0 r1-r4, 2.8.0r1, 2.5r6, 2.5 r1&2, 2.5, 2.6.1, 2.6.1 r1-r5, 2.7.1, 2.7.1 r1-r3, 2.10 r3&4, 3.0.1 r1	ScreenOS Remote Reboot	Low	CyberNotes-2002-11
NetScreen ¹⁴⁹²	Multiple	ScreenOS 3.0.3 r1.1	ScreenOS HTML File Display	Medium	CyberNotes-2002-12
NetScreen ¹⁴⁹³	Multiple	NetScreen-Remote Security Client 8.0, Remote VPN Client 8.0	NetScreen-Remote VPN Client IKE Packet Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-19
NetScreen Technologies Inc. ¹⁴⁹⁴	Multiple	ScreenOS 3.1.1r2, 3.1.0r9, 3.1.0r2, 3.1.0r1, 3.1.0, 3.0.0r1-r4, 3.0.0, 2.8.0r1, 2.7.1 r1-r3, 2.7.1, 3.0.1 r1&r2, 4.0	NetScreen Malicious URL Filter Bypassing	Medium	CyberNotes-2002-24
NetScreen Technologies Inc. ^{1495, 1496}	Multiple	ScreenOS 3.1.0, 3.0.0, 1.7, 2.6, 2.8, 4.0	ScreenOS Predictable Initial TCP Sequence Number	Medium	CyberNotes-2002-24
NetScreen Technologies Inc. ^{1497, 1498}	Multiple	ScreenOS 3.1.1r2, 3.1.0r9, 3.1.0r1&r2, 3.1.0, 3.0.0r1-r4, 3.0.0, 2.8.0r1, 2.8, 3.0.1r1&r2, 3.0.3 r1.1, 4.0	H.323 Control Session Denial Of Service	Low	CyberNotes-2002-24
NetScreen Technologies, Inc. ¹⁴⁹⁹	Windows 95/98/ME/NT 4.0/2000	ScreenOS 3.0.0- 3.0.0r3, 2.6.1- 2.6.1r4, 2.7.1-2.7.1r2	ScreenOS IP Spoof Protection Denial of Service	Low	CyberNotes-2002-03
Net-SNMP ¹⁵⁰⁰	Unix	Net-SNMP 4.2.3	Net-SNMP snmpnetstat Remote Heap Overflow	High	CyberNotes-2002-01

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Net-SNMP ¹⁵⁰¹	Unix	Net-SNMP 5.0.1, 5.0.3, 5.0.4 .pre2	Net-SNMP Denial of Service CVE Name: CAN-2002-1170	Low	CyberNotes-2002-20
NetWin ¹⁵⁰²	Multiple	WebNEWS 1.1j, 1.1i, 1.1h	WebNEWS Remote Buffer Overflow	High	CyberNotes-2002-04
NetWin ¹⁵⁰³	Multiple	WebNEWS 1.1k, 1.1j, 1.1i, 1.1h	WebNEWS Hard-Coded Programs	Medium	CyberNotes-2002-04
NetWin Limited ¹⁵⁰⁴	Windows 95/98/NT 4.0/2000, MacOS X 10.0, Unix	CWMail 2.7, 2.7a-2.7d, 2.7f, 2.7i-2.7q, 2.7s, 2.7t	CWMail.exe Buffer Overflow	High	CyberNotes-2002-04
Network Associates ¹⁵⁰⁵	Windows 95/98/ME/NT 4.0/2000	PGP 7.0, 7.0.3, 7.0.4	PGP Outlook Plug-In Insecure Message Storage	Medium	CyberNotes-2002-01
Network Associates ¹⁵⁰⁶	Windows 95/98/ME/NT 4.0/2000	PGP Security PGPfire 7.1	PGPFire TCP/IP Alteration	Medium	CyberNotes-2002-03
Network Associates ¹⁵⁰⁷	Windows 95/98/ME/NT 4.0/2000, XP, Apple MacOS 9.0	PGP Corporate Desktop 7.1, PGP Freeware 7.0.3, PGP Personal Security 7.0.3	Multiple PGP Products with Windows EFS Plaintext File Disclosure	Medium	CyberNotes-2002-10
Network Associates ¹⁵⁰⁸	Windows 95/98/ME/NT 4.0/2000, MacOS 9.0	Desktop Security 7.0.4, PGP Freeware 7.0.3, PGP Personal Security 7.0.3	PGP Outlook Plug-In Heap Corruption	High	CyberNotes-2002-14
Network Associates ¹⁵⁰⁹	Windows 95/98/NT 4.0/2000	PGP 7.0.4, 7.1	PGP Passphrase Cache Expiration	Medium	CyberNotes-2002-15
Network Associates ¹⁵¹⁰	Windows 95/98/ME/ NT 4.0/2000, MacOS 9.0	PGP Freeware 7.0.3	PGPFreeware Malformed IKE Response Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-17
Network Associates ¹⁵¹¹	Windows 95/98/ME/ NT 4.0/2000, Unix	PGP 5.0, 5.1i, 5.5.3i for Windows, 5.5.5, 6.0.2, 6.0.2i, 6.5.1i, 6.5.3i for Windows, 6.5.3, 6.5.8, 7.0, 7.0.3, 7.0.4, 7.1.1, PGP Corporate Desktop 7.1, 7.1.1, Freeware 7.0.3	PGP Desktop Filename Buffer Overflow CVE Name: CAN-2002-0850	High	CyberNotes-2002-18
Network Associates ¹⁵¹²	Windows 95/98/ME/ NT 4.0/2000, XP	McAfee VirusScan 4.5.1	VirusScan WebScanX Code Execution	High	CyberNotes-2002-25
Nevrona Designs ¹⁵¹³	Windows NT	MiraMail 1.04	MiraMail Plain Text Storage	Medium	CyberNotes-2002-02
New Atlanta ¹⁵¹⁴	Windows NT 4.0/2000	ServletExec/ISAPI 4.1	NewAtlanta Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained)	CyberNotes-2002-11
NEWLOG ¹⁵¹⁵	Windows 95/98/ME/NT 4.0/2000	NetSupport Manager 5.5, 6.10	NetSupport Manager Directory Traversal	Medium	CyberNotes-2002-07
Niels Chr Rød. Denmark ¹⁵¹⁶	Unix	Gender Mod 1.1.3	Gender Mod Administrative Access	High	CyberNotes-2002-16
Noah Grey ¹⁵¹⁷	Unix	Greymatter 1.2, 1.21b, 1.21a, 1.21	Greymatter Login/ Password Exposure	High	CyberNotes-2002-05
NOCC ¹⁵¹⁸	Multiple	NOCC 0.9-0.9.5	NOCC Webmail Script Injection	High	CyberNotes-2002-10
Noguska ¹⁵¹⁹	Unix	Nola 1.1.1, 1.1.2	Nola Remote File Include	High	CyberNotes-2002-13

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Nombas ¹⁵²⁰	Windows, OS/2, Unix	ScriptEase: Webserver Edition 4.30d win3.x, 4.30d OS/2, 4.30d NetWare 5, 4.30d ISAPI win32, 4.30d CGI/WINCGI win32, 4.30b Solaris, ppc, Linux, Irix, HP-UX; FreeBSD	ScriptEase: Webserver Edition Default Script	Medium	CyberNotes-2002-01
Nombas ¹⁵²¹	Windows, OS/2, Unix	ScriptEase: Webserver Edition 0.95 win3.x, Solaris, ppc, OS/2, NetWare 5, Linux, ISAPI win32, Irix, HP-UX, FreeBSD, CGIWINCGI win32	ScriptEase: WebServer Edition Multiple Denial of Service Vulnerabilities	Low	CyberNotes-2002-04
Nortel Networks ¹⁵²²	Unix	WebOS 9.0	WebOS Half-Closed Session	Medium	CyberNotes-2002-03
Nortel Networks ¹⁵²³	Multiple	CVX 1800 Multiservice Access Switch 3.6.3 p5, 3.6.3 p24	CVX 1800 Multi-Service Access Switch Default SNMP Community	Medium	CyberNotes-2002-08
Northern Solutions ¹⁵²⁴	Windows NT	Xeneo Web Server 2.0.759 .6, 2.1.0.0	Xeneo Web Server Remote Denial of Service CVE Name: CAN-2002-1248	Low	CyberNotes-2002-23
Novell ¹⁵²⁵	Multiple	GroupWise 6.0, Groupwise Enhancement Pack 5.5	GroupWise Servlet Gateway Default Authentication	Medium	CyberNotes-2002-01
Novell ¹⁵²⁶	Windows NT 4.0	NetWare 5.0, 5.0SP5, 5.1	NetWare Null Password	High	CyberNotes-2002-03
Novell ¹⁵²⁷	Windows	Groupwise 6.0	GroupWise LDAP Authentication Bypass	Medium	CyberNotes-2002-04
Novell ¹⁵²⁸	Windows	Groupwise 5.5	Novell GroupWise Web Access Path Disclosure	Medium	CyberNotes-2002-05
Novell ¹⁵²⁹	Multiple	NetWare 5.1, 6.0	NetWare Buffer Overflow	High	CyberNotes-2002-07
Novell ¹⁵³⁰	Multiple	Border Manager 3.5	Border Manager Connection Denial of Service	Low	CyberNotes-2002-10
Novell ¹⁵³¹	Multiple	Border Manager 3.6 SP1a	Border Manager Multiple Denial of Service Vulnerabilities	Low	CyberNotes-2002-10
Novell ¹⁵³²	Multiple	NetWare 5.1 SP4, 6.0 SP1	NetWare NWFTPD Denial of Service	Low	CyberNotes-2002-10
Novell ¹⁵³³	Multiple	eDirectory 8.6.2, 8.7	eDirectory Weak Password	Medium	CyberNotes-2002-12
Novell ¹⁵³⁴	Multiple	NetWare 6.0 SP1	NetWare DHCP Server Denial of Service	Low	CyberNotes-2002-13
Novell ¹⁵³⁵	Multiple	NetWare 6.0 SP1	NetWare NWFTPD Format String Remote Denial of Service	Low	CyberNotes-2002-13
Novell ¹⁵³⁶	Multiple	NetWare 6.0, 6.0 SP1	NetWare iManage Denial of Service	Low	CyberNotes-2002-13
Novell ¹⁵³⁷	Multiple	GroupWise 6.0, 6.0 SP1	GroupWise Internet Agent Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-15
Novell ¹⁵³⁸	Windows 95/98/ME/NT 4.0/2000, XP, Unix	NetMail 3.0.3, 3.1, XE 3.1	NetMail Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-15
Novell ¹⁵³⁹	Multiple	NetWare 5.1, 5.1 SP4, 6.0, 6.0 SP1	NetWare Buffer Overflow & Scripting Vulnerability	Medium	CyberNotes-2002-17
Novell ¹⁵⁴⁰	Multiple	NetWare 5.1, 5.1 SP4, 6.0, 6.0 SP1	NetWare Remote Perl Handler Vulnerabilities	High	CyberNotes-2002-17
Novell ¹⁵⁴¹	Multiple	NetWare 5.1, 6.0; Small Business Suite 5.1, 6.0	NetBasic Scripting Server Directory Traversal & Module Name Buffer Overflow	Medium/High (High if arbitrary code is executed)	CyberNotes-2002-17
Novell ¹⁵⁴²	Multiple	NetWare 6.0 SP2	NetWare RConsoleJ Secure IP Login	Medium	CyberNotes-2002-17
Novell ¹⁵⁴³	Multiple	eMFrame 1.2.1	eMFrame Buffer Overflow	Low	CyberNotes-2002-23

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Novell ^{1544, 1545}	Multiple	eDirectory 8.6.2, eDirectory Database 85.20, 85.24, 85.30	eDirectory Expired Password	Medium	CyberNotes-2002-23
NPDS ¹⁵⁴⁶	Multiple	NPDS 4.8	NPDS News Message HTML Injection	High	CyberNotes-2002-20
NullLogic ¹⁵⁴⁷	Multiple	Null HTTPd 0.5	Null HTTPd Error Page Cross-Site Scripting	High	CyberNotes-2002-18
NullLogic ¹⁵⁴⁸	Windows, Unix	Null HTTPd 0.5	Null HTTPd Remote Heap Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-20
NullLogic ¹⁵⁴⁹	Multiple	Null HTTPd 0.5, 0.5.1	Null HTTPD Remote Heap Corruption	High	CyberNotes-2002-24
nullmailer ¹⁵⁵⁰	Unix	nullmailer 1.0 RC5	Nullmailer Invalid User Denial Of Service	Low	CyberNotes-2002-24
NullSoft ¹⁵⁵¹	Windows 95/98/ME/NT 4.0/2000, XP	Winamp 2.79	Winamp Minibrowser Buffer Overflow	High	CyberNotes-2002-09
NullSoft ¹⁵⁵²	Windows 95/98/ME/NT 4.0/2000	Winamp 2.80	Winamp Plaintext Authentication	Medium	CyberNotes-2002-11
NullSoft ¹⁵⁵³	Unix	Shoutcast Server 1.8.9 Win32, Solaris, Mac OS X, Linux, FreeBSD	Shoutcast Remote Buffer Overflow	High	CyberNotes-2002-12
NullSoft ¹⁵⁵⁴	Windows 95/98/ME/NT 4.0/2000, XP	Winamp 2.50, 2.60 (lite), (full), 2.61 (full), 2.62 (standard), 2.64 (standard), 2.65, 2.70, 2.70 (full), 2.71, 2.72, 2.73-2.80, 2.73 (full)	Winamp Buffer Overflow	High	CyberNotes-2002-14
NullSoft ¹⁵⁵⁵	Windows 95/98/ME/NT 4.0/2000, XP	Winamp 2.65, 2.70-2.80	Winamp Skin Predictable File Location	High	CyberNotes-2002-15
NullSoft ¹⁵⁵⁶	MacOS X, Unix	Shoutcast Server 1.8.9 Solaris, Mac OS X, Linux, FreeBSD	Shoutcast Insecure Permissions	Medium	CyberNotes-2002-16
NullSoft ¹⁵⁵⁷	Windows 95/98/ME/NT 4.0/2000, XP	WinAmp 2.76, 2.79	WinAmp Playlist Cross-Site Scripting	High	CyberNotes-2002-16
NullSoft ¹⁵⁵⁸	Windows ME	Winamp 3.0	Winamp Skin File Buffer Overflow	High	CyberNotes-2002-20
NullSoft ¹⁵⁵⁹	Windows 95/98/ME/NT 4.0/2000	Shoutcast Server 1.8.3 Win32	Shoutcast 'Admin.CGI' Denial of Service	Low	CyberNotes-2002-02
Nylon ¹⁵⁶⁰	Unix	Nylon 0.2	Nylon Proxy Receive Function Remote Denial of Service	Low	CyberNotes-2002-21
Oblix ¹⁵⁶¹	Windows NT 4.0/2000, Unix	NetPoint 5.2	NetPoint Account Lock Bypass	Medium	CyberNotes-2002-06
Oddsock ¹⁵⁶²	Windows 95/98/NT 4.0/2000, XP	Song Requester 2.1	Song Requester WinAmp Plugin Denial of Service	Low	CyberNotes-2002-15
Olaf Titz ^{1563, 1564}	Unix	CIPE 1.0.1, 1.1, 1.2, 1.3, 1.4.5, 1.4.6, 1.5.2	CIPE Denial of Service CVE Name: CAN-2002-0047	Low	CyberNotes-2002-02
Oliver Rauch ¹⁵⁶⁵	Unix	xSANE 0.81	xSANE Insecure Temporary File Creation CVE Name: CAN-2001-0887	Medium	CyberNotes-2002-01
Omnicon Technologies Corporation ¹⁵⁶⁶	Windows 95/98/NT 4.0/2000, XP	Omni HTTPD 1.1, 2.0 Alpha 1&2, 2.0.9, 2.0.4-2.0.8, 2.4 Pro	OmniHTTPD Sample Scripts Cross-Site Scripting	High	CyberNotes-2002-18
Omnicon Technologies Corporation ¹⁵⁶⁷	Windows 95/98/NT 4.0/2000, XP	Omni HTTPD 1.1, 2.0 Alpha 1&2, 2.0.9, 2.0.4-2.0.8, 2.4 Pro	OmniHTTPD Sample Application HTML Injection	High	CyberNotes-2002-18

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Omnicon Technologies Corporation ¹⁵⁶⁸	Windows 95/98/NT 4.0/2000, XXP	Omni HTTPD 2.0 9	OmniHTTPD Long Request Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-14
onlinetools.org ¹⁵⁶⁹	Unix	PHPImage View 1.0	PHPImage View Cross-Site Scripting & Information Disclosure	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-10
Open LDAP ¹⁵⁷⁰	Unix	OpenLDAP 2.0- 2.0.23	OpenLDAP Multiple Buffer Overflow	High	CyberNotes-2002-25
Open Office ¹⁵⁷¹	Windows, Unix	OpenOffice 1.0.1	OpenOffice Installation Insecure Temporary File Creation	Medium	CyberNotes-2002-21
Open Webmail ¹⁵⁷²	Unix	Open Webmail 1.70, 1.71	Open WebMail Invalid Username	Medium	CyberNotes-2002-24
OpenBB ¹⁵⁷³	Multiple	OpenBB 1.0.beta 1, RC1&RC2	OpenBB Cross-Site Scripting	High	CyberNotes-2002-05
OpenBB ¹⁵⁷⁴	Multiple	OpenBB 1.0.0 RC1-RC3	OpenBB Unauthorized Access	High	CyberNotes-2002-11
OpenBB ¹⁵⁷⁵	Multiple	OpenBB 1.0.0 RC3	OpenBB BBCode HTML Injection	High	CyberNotes-2002-11
OpenBB ¹⁵⁷⁶	Multiple	OpenBB 1.0.0 RC3	OpenBB Cross-Site Scripting	High	CyberNotes-2002-11
OpenBSD ¹⁵⁷⁷	Unix	OpenBSD 3.0	OpenBSD Authentication	Medium	CyberNotes-2002-06
OpenBSD ¹⁵⁷⁸	Unix	OpenBSD 3.0	OpenBSD PF Fingerprinting	Medium	CyberNotes-2002-07
OpenBSD ¹⁵⁷⁹	Unix	OpenBSD 2.9, 3.0	OpenBSD Root Compromise	High	CyberNotes-2002-08
OpenBSD ¹⁵⁸⁰	Unix	OpenBSD 2.4-2.9, 3.0, 3.1	OpenBSD exec C Library Standard I/O File Descriptor Race Condition	High	CyberNotes-2002-10
OpenBSD ¹⁵⁸¹	Unix	OpenBSD 3.1	OpenBSD SSHD Authentication	Medium	CyberNotes-2002-11
OpenBSD ¹⁵⁸²	Unix	OpenBSD 3.0, 3.1	OpenBSD select() Buffer Overflow	High	CyberNotes-2002-17
OpenBSD ¹⁵⁸³	Unix	OpenBSD 2.0-3.1	OpenBSD setitimer(2) Kernel Memory Overwrite	High	CyberNotes-2002-20
OpenBSD ¹⁵⁸⁴	Unix	OpenBSD 3.0, 3.1	OpenBSD getrlimit(2) Denial of Service	Low	CyberNotes-2002-23
OpenBSD ¹⁵⁸⁵	Unix	OpenBSD 2.9-3.2	OpenBSD False syslogd Source IP Reporting	Medium	CyberNotes-2002-24
OpenLDAP ¹⁵⁸⁶	Unix	OpenLDAP 2.0-2.0.7	OpenLDAP Object Attribute Deletion and Access Control Permissions	Medium	CyberNotes-2002-02
OpenSSH ¹⁵⁸⁷	Unix	OpenSSH 2.1, 2.1.1, 2.2, 2.3, 2.5, 2.5.1, 2.5.2, 2.9 p2, 2.9 p1, 2.9, 2.9.9, 3.0, 3.0.1, 3.0.2, 3.1, 3.2	OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow	Medium	CyberNotes-2002-09
OpenSSH ¹⁵⁸⁸	MacOS X 10.x, Unix	OpenSSH 3.2.2 p1, 3.4 p1, 3.4	OpenSSH Trojan Horse	High	CyberNotes-2002-16
OpenSSH ¹⁵⁸⁹	Unix	OpenSSH	OpenSSH Visible Password	Medium	CyberNotes-2002-23
OpenSSL Project ^{1590, 1591, 1592, 1593, 1594, 1595, 1596, 1597, 1598, 1599} <i>New Internet worm circulating that exploits the SSLv2 handshake vulnerability</i> ¹⁶⁰⁰	Unix	OpenSSL 0.9.7 beta1&2	Multiple OpenSSL Vulnerabilities CVE Name: CAN-2002-0655, CAN-2002-0656, CAN-2002-0657	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-16 CyberNotes-2002-19
OpenSSL Project ^{1601, 1602, 1603, 1604, 1605, 1606, 1607, 1608, 1609, 1610, 1611, 1612, 1613}	Windows NT 4.0, MacOS X 10.x, Unix	Apple MacOS X 10.0x; OpenSSL Project OpenSSL 0.9.1c, 0.9.2b, 0.9.3-0.9.7; Oracle Corporate Time Outlook Connector 3.1-3.1.2, 3.3, Oracle 9i Application Server 1.0.2.2, 1.0.2.1s, 1.0.2, Oracle HTTP Server 9.0.1, 9.2.0	OpenSSL ASN.1 Parsing Error Denial of Service CVE Name: CAN-2002-0659	Low	CyberNotes-2002-16
Openwall Project ¹⁶¹⁴	Unix	Linux kernel 2.4.18 x86	Linux kernel IPC Signal Handling	Medium	CyberNotes-2002-06

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Opera Software ¹⁶¹⁵	Windows 95/98/ME/NT 4.0/2000, XP	Opera Web Browser 6.0.1 win32	Opera Content-Type HTML File Execution	High	CyberNotes-2002-04
Opera Software ¹⁶¹⁶	Windows 95/98/ME/NT 4.0/2000, XP	Opera Web Browser 5.12, 5.12 win32, 6.0, 6.0 win32, 6.0.1, 6.0.1 win32	Opera Frame Location Same Origin Policy Bypass	High	CyberNotes-2002-10
Opera Software ¹⁶¹⁷	Windows 95/98/ME/NT 4.0/2000, XP	Opera Web Browser 6.0.1 win32, 6.0.2 win32	Opera Arbitrary File Disclosure	Medium	CyberNotes-2002-11
Opera Software ¹⁶¹⁸	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Opera Web Browser 6.0, 6.0 win32, 6.0.1, 6.0.1 win32, 6.0.1 Linux, 6.0.2 win32- 6.0.4 win32	Opera Cross-Site Scripting	High	CyberNotes-2002-16
Opera Software ¹⁶¹⁹	Unix	Opera Web Browser 6.0.1 Linux	Opera Oversized Image Width Denial of Service	Low	CyberNotes-2002-19
Opera Software ¹⁶²⁰	Unix	Opera Web Browser 6.0.3 Linux	Opera HTTPS Proxy Denial of Service	Low	CyberNotes-2002-24
Opera Software ¹⁶²¹	Windows, MacOS, Unix	Opera Web Browser 7.0 win32 Beta 1	Multiple Unspecified Opera 7 Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-24
Oracle Corporation ¹⁶²²	Windows NT 4.0/2000, Unix	Oracle 9i Application Server	Oracle 9i Application Server PL/SQL Apache Module Buffer Overflow and Directory Traversal	Medium/High (High for the PL/SQL buffer overflow vulnerability.)	CyberNotes-2002-01
Oracle Corporation ¹⁶²³	Windows NT 4.0/2000, Unix	Oracle9iAS Web Cache 2.0.0.0-2.0.0.2, 2.0.0.2 NT	Oracle9iAS Web Cache Multiple Vulnerabilities	Low/ Medium	CyberNotes-2002-01
Oracle Corporation ¹⁶²⁴	Multiple	Oracle8i 8.0.1, 8.0.2, 8.0.4-8.0.6, 8.1.5- 8.1.7.1	Oracle 8i Remote Denial of Service	Low	CyberNotes-2002-02
Oracle Corporation ¹⁶²⁵	Multiple	Oracle8i 8.0.1, 8.0.2, 8.0.4-8.0.6, 8.1.5- 8.1.7.1, Oracle9i 9.0, 9.0.1	Oracle RDBMS Demo Account	Medium	CyberNotes-2002-02
Oracle Corporation ¹⁶²⁶	Multiple	Oracle8i 8.0.2, 8.0.4-8.0.6, 8.1.5- 8.1.7.1, Oracle9i 9.0, 9.0.1	Oracle SQL*Plus Default Settings	High	CyberNotes-2002-02
Oracle Corporation ¹⁶²⁷	Multiple	Oracle8i 8.0.2, 8.0.4-8.0.6, 8.1.5- 8.1.7.1, Oracle9i 9.0, 9.0.1	Oracle Default Auditing Configuration	Medium	CyberNotes-2002-02
Oracle Corporation ¹⁶²⁸	Multiple	Oracle database server 8.1.7.0.0, Oracle 8i Enterprise Edition 8.0.5.0.0, 8.0.6.0.1, 8.0.6.0.0, 8.1.5.1.0, 8.1.5.0.2, 8.1.5.0.0, 8.1.6.1.0, 8.1.6.0.0, 8.1.7.1.0, 8.1.7.0.0, Oracle8 8.0.3, 8.0.4, 8.0.5.1, 8.0.5, 8.0.6, 8.1.5-8.1.7, 8.0.1, 8.0.2, 8.0.4-8.0.6, 8.1.5-8.1.7.1, 9.0, 9.0.1	Oracle TNS Listener Arbitrary Function	High	CyberNotes-2002-03
Oracle Corporation ¹⁶²⁹	Multiple	Oracle9i 9.0, 9.0.1, Oracle9iAS Web Cache 2.0.0.0- 2.0.0.3	Oracle 9iAS .java Source Code	Medium	CyberNotes-2002-03
Oracle Corporation ¹⁶³⁰	Windows NT 4.0/2000, Unix	Oracle9i 9.0, 9.0.1, Oracle9iAS Web Cache 2.0.0.3, 2.0.0.3, 2.0.0.2 NT, 2.0.0.2, 2.0.0.1, 2.0.0.0	Oracle 9iAS Denial of Service & Buffer Overflow Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-03
Oracle Corporation ¹⁶³¹	Windows NT 4.0/2000, Unix	Oracle 9i Application Server 0.0	Oracle Default Passwords	Medium	CyberNotes-2002-06
Oracle Corporation ¹⁶³²	Windows NT 4.0/2000, Unix	Oracle 9i Application Server 0.0	Oracle 9iAS PL/SQL OWA_UTIL Procedure Exposure	Medium	CyberNotes-2002-06

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Oracle Corporation ¹⁶³³	Multiple	Oracle 9i Application Server 1.0.2, Oracle8i 8.1.7, 8.1.7.1, Oracle9i 9.0, 9.0.1	Oracle 9i Default Configuration File Information Disclosure	Medium	CyberNotes-2002-06
Oracle Corporation ¹⁶³⁴	Multiple	Oracle9iAS Web Cache 2.0.0.0-2.0.0.3, Oracle9i 9.0, 9.1, Oracle8i 8.1.7, 8.1.7.1, Oracle 9i Application Server 1.0.2	Oracle 9iAS Web Administration Access	High	CyberNotes-2002-06
Oracle Corporation ¹⁶³⁵	Multiple	Oracle Configurator 11.0 i	Oracle Configurator Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-07
Oracle Corporation ¹⁶³⁶	Unix	Oracle8i 8.1.5	Oracle 8i TNS Listener Local Buffer Overflow	High	CyberNotes-2002-07
Oracle Corporation ¹⁶³⁷	Multiple	Oracle9i 9.0, 9.0.1	Oracle 9i TNS Denial of Service	Low	CyberNotes-2002-07
Oracle Corporation ¹⁶³⁸	Multiple	Oracle9i 9.0, 9.0.1	Oracle 9i ANSI Outer Join Access Control Bypass	Medium	CyberNotes-2002-08
Oracle Corporation ¹⁶³⁹	Multiple	Oracle Reports6i 6.0.8, 6.0.8.19, Oracle9iAS Reports 9.0.2	Oracle Reports Server Information Disclosure	Medium	CyberNotes-2002-15
Oracle Corporation ¹⁶⁴⁰	Multiple	Oracle 9i Application Server 1.0.2.2, 1.0.2.1s, 1.0.2, 9.0.2	Oracle 9iAS OJSP Demo Scripts Cross-Site Scripting	High	CyberNotes-2002-17
Oracle Corporation ¹⁶⁴¹	Multiple	Oracle8i 8.1.5- 8.1.7.1, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Release 2 9.2.2, 9.2.1	Oracle Net Listener Format String	Medium	CyberNotes-2002-17
Oracle Corporation ¹⁶⁴²	Multiple	Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.1	Oracle Listener Remote Denial of Service CVE Name: CAN-2002-0856	Low	CyberNotes-2002-17
Oracle Corporation ¹⁶⁴³	Multiple	E-Business Suite 11i 11.1-11.6	E-Business Suite Authentication Bypassing	Medium	CyberNotes-2002-21
Oracle Corporation ¹⁶⁴⁴	Multiple	Oracle 8i Enterprise Edition 8.1.5.1.0, 8.1.5.0.2, 8.1.5.0.0, 8.1.6.1.0, 8.1.6.0.0, 8.1.7.1.0, 8.1.7.0.0, Oracle8i 8.1.5, 8.1.6, 8.1.7.1, 8.1.7, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	Oracle TNS Listener Service_CurLoad Remote Denial of Service CVE Name: CAN-2002-1118	Low	CyberNotes-2002-21
Oracle Corporation ¹⁶⁴⁵	Windows	Oracle 9i Application Server 9.0.2	Oracle 9i Application Server Remote Denial of Service	Low	CyberNotes-2002-21
Oracle Corporation ¹⁶⁴⁶	Windows NT 4.0/2000, XP, Unix	Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	Oracle 9i Database Server Malformed USERID Buffer Overflow	Medium	CyberNotes-2002-22
Organic PHP ¹⁶⁴⁷	Multiple	PHP-Affiliate 1.0	PHP-Affiliate 'Details.PHP' Authentication Bypassing	Medium	CyberNotes-2002-17
Os Commerce ¹⁶⁴⁸	Multiple	Os Commerce 2.1	OSCommerce Arbitrary Code Execution	High	CyberNotes-2002-13
Outfront ¹⁶⁴⁹	Windows NT	Spooky Login 2.0-2.5	Spooky Login Password Manipulation	Medium	CyberNotes-2002-09
Pablo Software Solutions ¹⁶⁵⁰	Windows 98/NT 4.0, XP	FTP Server 1.0	FTP Server Directory Traversal	Medium	CyberNotes-2002-15
Pablo Software Solutions ¹⁶⁵¹	Windows 98/NT 4.0/2000, XP	FTP Server 1.0, 1.2, 1.3, 1.5	FTP Server Format String CVE Name: CAN-2002-1244	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-23
Pacific Software ¹⁶⁵²	Multiple	Carello 1.3	Carello Shopping Cart Remote File Execution	High	CyberNotes-2002-14
Padl Software Pty Ltd ¹⁶⁵³	Unix	nss_ldap Build 85, 105, 107, 113, 121, 172, 173, 180, 181, 183-192, 194	nss_ldap DNS Buffer Overflow & Denial of Service CVE Name: CAN-2002-0825	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-23

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
PaintBBS ¹⁶⁵⁴	Multiple	PaintBBS 1.2	PaintBBS Configuration File & 'cgi-bin' Directory	High	CyberNotes-2002-02
ParaChat ¹⁶⁵⁵	Multiple	ParaChat Server 4.0	ParaChat Denial of Service	Low	CyberNotes-2002-16
PascaL Michaud ¹⁶⁵⁶	Windows NT	ASP Client Check 1.3, 1.5	ASP Client Authentication Bypass	Medium	CyberNotes-2002-10
Patrick Powell ¹⁶⁵⁷	Unix	LPRng 3.7.4, 3.8.9	LPRNG Remote Print Submission CVE Name: CAN-2002-0378	Low	CyberNotes-2002-12
Paul Kulchenko ¹⁶⁵⁸	Unix	SOAP::Lite	SOAP::Lite Remote Arbitrary Command Execution	High	CyberNotes-2002-08
Pedestal Software ¹⁶⁵⁹	Windows NT 4.0/2000	Integrity Protection Driver 1.2	Integrity Protection Driver Bypass	Medium	CyberNotes-2002-25
Perception ¹⁶⁶⁰	Windows	LiteServe 2.0.1	LiteServe Input Validation Vulnerabilities	High	CyberNotes-2002-23
Perception ¹⁶⁶¹	Multiple	LiteServe 2.0.1	LiteServe Cross-Site Scripting	High	CyberNotes-2002-23
Perception ¹⁶⁶²	Windows NT	LiteServe 2.0, 2.0.1, 2.0.2	LiteServe CGI Source Disclosure	Medium	CyberNotes-2002-24
Perception ¹⁶⁶³	Windows NT	LiteServe 2.0, 2.0.1, 2.0.2	LiteServe Malformed GET Request Buffer Overflow	Low	CyberNotes-2002-24
Perception Software ¹⁶⁶⁴	Windows 98/2000	LiteServe 2.0	LiteServe Authentication Bypass	Medium	CyberNotes-2002-22
Perlbot ¹⁶⁶⁵	Windows, Unix	Perlbot 1.0 beta	Perlbot E-mail Sending Remote Command Execution	High	CyberNotes-2002-22
Perlbot ¹⁶⁶⁶	Windows, Unix	Perlbot 1.0 beta	Perlbot Arbitrary Shell Script	High	CyberNotes-2002-22
Perlbot ¹⁶⁶⁷	Windows, Unix	Perlbot 1.9.2	Perlbot Remote Command Execution Vulnerabilities	High	CyberNotes-2002-22
Peter Sandvik ¹⁶⁶⁸	Unix	Simple Web Server 0.5.1	Simple Web Server File Disclosure CVE Name: CAN-2002-1238	Medium	CyberNotes-2002-23
PFinger ¹⁶⁶⁹	Unix	PFinger 0.7.5-0.7.7	PFinger Format String	High	CyberNotes-2002-01
Philip Chinery ¹⁶⁷⁰	Multiple	Guestbook 1.1	Guestbook Script Injection	High	CyberNotes-2002-09
Phorum ¹⁶⁷¹	Unix	Phorum 3.3.2	Phorum Sensitive Information	Medium	CyberNotes-2002-05
Phorum ¹⁶⁷²	Multiple	Phorum 3.3.2 a	Phorum Script Injection	High	CyberNotes-2002-10
Phorum ¹⁶⁷³	Unix	Phorum 3.3.2 a	Phorum Remote Command Execution	High	CyberNotes-2002-11
Phorum ¹⁶⁷⁴	Multiple	Phorum 3.3.2 a, 3.3.2	Phorum Cross-Site Scripting	High	CyberNotes-2002-11
PHP ¹⁶⁷⁵	Multiple	PHP 3.0- 3.0.13, 3.0.16, 4.0, 4.0.1p12, 4.0.1, 4.0.3-4.0.6, 4.1, 4.1.1	PHP MySQL Safe_Mode Filesystem Circumvention	High	CyberNotes-2002-03
PHP ¹⁶⁷⁶	Multiple	FirstPost PHP FirstPost 0.1	FirstPost Path Disclosure	Medium	CyberNotes-2002-06
PHP ¹⁶⁷⁷	Multiple	Gratuit Recherche 1.3	Recherche Cross-Site Scripting	High	CyberNotes-2002-09
PHP ¹⁶⁷⁸	Unix	PHP 4.0-4.0.7, 4.1.0-4.1.2	PHP posix_getpwnam / posix_getpwuid safe_mode Circumvention	Medium	CyberNotes-2002-09
PHP ¹⁶⁷⁹	MacOS X 10.0x, Unix	PHP 3.0, 3.0.10 -3.0.18, 3.0.1-3.0.13, 3.0.16, 4.0- 4.0.7 RC3, 4.1.0-4.1.2, 4.2.0-4.2.2	PHP Interpreter Denial of Service	Low	CyberNotes-2002-15
PHP ¹⁶⁸⁰	Multiple	PHP 4.2.0 4.2.1	PHP HTTP POST Incorrect MIME Header Parsing	High	CyberNotes-2002-15
PHP ¹⁶⁸¹	Unix	PHP 4.2.3	PHP Header Function Script Injection	High	CyberNotes-2002-19
PHP Arena ¹⁶⁸²	Windows, Unix	paFileDB 1.1.3, 2.1.1	paFileDB Search Cross-Site Scripting	High	CyberNotes-2002-22
PHP Arena ¹⁶⁸³	Windows, Unix	paFileDB 1.1.3, 2.1.1, 3.0	paFileDB Multiple Cross-Site Scripting	High	CyberNotes-2002-22
PHP Auction ¹⁶⁸⁴	Multiple	PHP Auction 1.2, 1.3, 2.0, 2.1	PHPAuction Unauthorized Administrative Access	Medium	CyberNotes-2002-14
PHP Development Team ¹⁶⁸⁵	Multiple	PHP 4.0, 4.0.1p12, 4.0.1, 4.0.3-4.0.6, 4.1, 4.1.1	PHP or JSP Include File Sensitive Information Disclosure	Medium	CyberNotes-2002-04

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
PHP Development Team ¹⁶⁸⁶	Unix, MacOS X 10.x	PHP 4.0, 4.0.1 p12, 4.0.1 p11, 4.0.1, 4.0.2, 4.0.3 p11, 4.0.3-4.0.7, 4.1.0, 4.1.1, 4.1.2, 4.2.0-4.2.2	PHP Mail Function ASCII Control Character Header Spoofing CVE Name: CAN-2002-0986	Medium/High (High if arbitrary code is executed)	CyberNotes-2002-18
PHP Evolution ¹⁶⁸⁷	Unix	News Evolution 1.0, 2.0	News Evolution Include Undefined Variable Command Execution	Medium High (High if arbitrary code can be executed)	CyberNotes-2002-24
PHP Group ¹⁶⁸⁸	Unix	PHP 4.0.4- 4.0.6, 4.1- 4.1.1	PHP4 Session IDs	High	CyberNotes-2002-02
PHP ^{1689, 1690, 1691} <i>RedHat releases patch¹⁶⁹²</i>	MacOS X 10.x, Unix	PHP 3.0.14-3.0.18, 4.0.3-4.0.7, 4.1.0- 4.1.2, 4.2.0-4.2.3	PHP Function fopen() CRLF Injection CVE Name: CAN-2002-0985	Medium	CyberNotes-2002-19 CyberNotes-2002-23
PHP-Address ¹⁶⁹³	Unix	PHP-Address 0.2e	PHP-Address Remote File Include	High	CyberNotes-2002-13
phpBB Group ¹⁶⁹⁴	Unix	phpBB 1.0 .0, 1.2 .0, 1.2.1, 1.4 .0, 1.4.1, 1.4.2, 1.4.4	phpBB Image Tag User-Embedded Scripting	High	CyberNotes-2002-07
phpBB Group ¹⁶⁹⁵	Multiple	phpBB 1.0.0, 1.2.0, 1.2.1, 1.4.0, 1.4.1, 1.4.2, 1.4.4	phpBB BBCode Denial Of Service & Database Corruption	Low	CyberNotes-2002-07
phpBB Group ¹⁶⁹⁶	Multiple	phpBB 2.0 Beta 1, 2.0 RC1-RC3	phpBB2 Remote Extension Command	High	CyberNotes-2002-07
phpBB Group ¹⁶⁹⁷	Multiple	phpBB 2.0.0, 2.0 RC1-RC4, 2.0 Beta 1	PHPBB2 Image Tag HTML Injection	High	CyberNotes-2002-11
phpBB Group ¹⁶⁹⁸	Multiple	phpBB 2.0.0, 2.0 RC1-4, 2.0.1	PHPBB2 Install.PHP Remote File Include	High	CyberNotes-2002-13
phpBB Group ¹⁶⁹⁹	Multiple	phpBB 2.0.0-2.0.3	PHPBB2 Avatar Information Disclosure	Medium	CyberNotes-2002-21
phpBB Group ¹⁷⁰⁰	Unix	phpBB 2.0.0	phpBB2 Unauthorized Administrative Access	High	CyberNotes-2002-22
phpBB Group ¹⁷⁰¹	Unix	phpBB 2.0.3	PHPBB2 ViewTopic. PHP Cross-Site Scripting	High	CyberNotes-2002-24
phpBB Group ¹⁷⁰²	Unix	phpBB 2.0.3	phpBB Forum Postings	High	CyberNotes-2002-24
phpBB Group ¹⁷⁰³	Unix	phpBB 2.0.3	phpBB Cross-Site Scripting	High	CyberNotes-2002-25
phpBB mod ¹⁷⁰⁴	Windows, Unix	phpBBmod 1.3.3	PHPBBMod PHPInfo Information Disclosure	Medium	CyberNotes-2002-21
phpGB ¹⁷⁰⁵	Unix	phpGB 1.1	phpGB HTML Injection	High	CyberNotes-2002-19
phpGB ¹⁷⁰⁶	Unix	phpGB 1.1, 1.2	phpGB PHP Code Injection	High	CyberNotes-2002-19
phpGB ¹⁷⁰⁷	Unix	phpGB 1.1, 1.2, 1.3	phpGB SQL Injection	Medium/ High (High if administrative privileges are obtained)	CyberNotes-2002-19
PHPGroupWare ¹⁷⁰⁸	Multiple	PHPGroupWare 0.9.12	PHPGroupWare Login SQL Command Execution	High	CyberNotes-2002-07
phpLinkat ¹⁷⁰⁹	Windows, Unix	phpLinkat 0.1 .0	phpLinkat Multiple Cross Site Scripting	High	CyberNotes-2002-21
phpMy News Letter ¹⁷¹⁰	Unix	phpMy NewsLetter 0.6.10	phpMyNews Letter Remote File Include	High	CyberNotes-2002-20
PHPNet Toolpack ¹⁷¹¹	Unix	PHPNetToolpack 0.1	PHPNet Toolpack Input Validation	High	CyberNotes-2002-06
PHPProjekt ¹⁷¹²	Multiple	PHPProjekt 2.0-3.1	PHPProjekt Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-09
PHPProjekt Development Team ¹⁷¹³	Unix	PHPProjekt 3.1, 3.1a	PHPProjekt Permissions	High	CyberNotes-2002-06

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
phpRank ¹⁷¹⁴	Windows, Unix	phpRank 1.8	PHPRank Multiple Remote Vulnerabilities	Medium High (High if arbitrary code can be executed)	CyberNotes-2002-21
PHP-Reactor ¹⁷¹⁵	Multiple	Ekilat LLC php(Reactor) 1.2.7	Global.INC. PHP Cross-Site Scripting	High	CyberNotes-2002-12
PhpSms Send ¹⁷¹⁶	Multiple	PhpSmsSend 1.0	PhpSmsSend Remote Arbitrary Command	High	CyberNotes-2002-03
PHP-Survey ¹⁷¹⁷	Unix	PHP-Survey prebeta-20000327, 20000615, 20000614b, 20000614, 20000421, 20000420	PHP-Survey Information Disclosure	Medium	CyberNotes-2002-09
PhpWeb Gallery ¹⁷¹⁸	Multiple	PhpWeb Gallery 1.0	PhpWeb Gallery Cookie Manipulation Compromise	High	CyberNotes-2002-09
PhpWeb Things ¹⁷¹⁹	Multiple	PhpWeb Things 0.4	PHPWeb 'core/main.php' Script	Medium	CyberNotes-2002-03
PHP-Wiki ¹⁷²⁰	Multiple	PHP-Wiki 1.2, 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3	PHP-Wiki Cross-Site Scripting	High	CyberNotes-2002-15
Phystech ¹⁷²¹	Unix	dhcpd 1.3.22 -p11	DHCPD Character Expansion Remote Command Execution	High	CyberNotes-2002-24
Pingtel ¹⁷²²	Multiple	Expressa 1.2.5, 1.2.7.4	Expressa VoIP phones Multiple Vulnerabilities CVE Names: CAN-2002-0667, CAN-2002-0668, CAN-2002-0669, CAN-2002-0670, CAN-2002-0671, CAN-2002-0672, CAN-2002-0673, CAN-2002-0674, CAN-2002-0675	High	CyberNotes-2002-15
Pingtel ¹⁷²³	Multiple	Xpressa 1.2.5, 1.2.7.4, 1.2.8, 2.0, 2.0.1	Xpressa Phone Multiple Vulnerabilities	Medium	CyberNotes-2002-17
Pirch IRC ¹⁷²⁴	Windows	Pirch IRC 98	Pirch IRC Link Handling Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-13
Pi-Soft ¹⁷²⁵	Windows 95/98/ME/NT 4.0/2000	SpoonFTP 1.1.0.1, 1.00.13, 1.00.12, 1.0, 1.1	SpoonFTP 'PORT' Command	Medium	CyberNotes-2002-02
Planet DNS ¹⁷²⁶	Window NT	PlanetWeb 1.14	PlanetWeb Long GET Request Buffer Overflow	High	CyberNotes-2002-19
pIDaniels ¹⁷²⁷	Unix	RipMime 1.2.0-1.2.6	RipMime Filename Buffer Overflow	High	CyberNotes-2002-02
Plesk ¹⁷²⁸	Unix	Plesk Server Administrator 1.0	Plesk Server Administrator PHP Source Disclosure	Medium	CyberNotes-2002-01
Plumtree ¹⁷²⁹	Multiple	Plumtree Corporate Portal 4.5	Plumtree Corporate Portal Cross-Site Scripting	High	CyberNotes-2002-01
Pointsec Mobile Technologies ¹⁷³⁰	Multiple	PalmOS 1.0 1.1	PalmOS PIN Disclosure	Medium	CyberNotes-2002-10
Polycom ¹⁷³¹	Multiple	View Station 128 6.5.1, 7.2, 512 6 5.1, 7.2, DCP 6.5.1, 7.2, FX/VS 4000 4.1.5, H.323 6.5.1, 7.2, MP 6.5.1, 7.2, SP/SP384 6.5.1, 7.2, V.35 6.5.1, 7.2	ViewStation Multiple Vulnerabilities CVE Names: CAN-2002-0626, CAN-2002-0627, CAN-2002-0628, CAN-2002-0629, CAN-2002-0630	Low/ Medium/High (Medium if sensitive information is obtained or unauthorized access is obtained) (High if the administrator password is obtained)	CyberNotes-2002-18

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Polycom ¹⁷³²	Multiple	ViaVideo 2.2, 3.0	ViaVideo Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-21
PortailPHP ¹⁷³³	Unix	PortailPHP 0.99	PortailPHP SQL Injection	Medium	CyberNotes-2002-24
Portix-PHP ¹⁷³⁴	Unix	Portix-PHP 0.4.02, 0.4.0	Portix-PHP Cookie Manipulation	High	CyberNotes-2002-03
Portix-PHP ¹⁷³⁵	Unix	Portix-PHP 0.4.02, 0.4.0	Portix-PHP 'view.php' and 'index.php' Directory Traversal Vulnerabilities	Medium	CyberNotes-2002-03
Posadis ¹⁷³⁶	Unix	Posadis m5pre1	Posadis DNS Server Format String	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-07
Post Calendar Development Team ¹⁷³⁷	Multiple	Post Calendar 3.0	PostCalendar Cross-Site Scripting	High	CyberNotes-2002-09
PostBoard ¹⁷³⁸	Unix	PostBoard 2.0, 2.0.1	PostBoard Multiple Vulnerabilities	Low/High (High if arbitrary script code can be executed)	CyberNotes-2002-09
Postgre SQL ¹⁷³⁹	Multiple	Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2	PostgreSQL cash_words Buffer Overflow	High	CyberNotes-2002-17
Postgre SQL ¹⁷⁴⁰	Multiple	Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1	PostgreSQL Repeat Function Buffer Overflow	High	CyberNotes-2002-17
Postgre SQL ¹⁷⁴¹	Multiple	Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1	PostgreSQL lpad() & rpad() functions Buffer Overflow	Low	CyberNotes-2002-17
PostNuke Development Team ¹⁷⁴²	Multiple	PostNuke 0.7.0.3	PostNuke Remote Command Execution	High	CyberNotes-2002-07
PostNuke Development Team ¹⁷⁴³	Multiple	PostNuke 7.0.3 & prior	PostNuke Cross-Site Scripting	High	CyberNotes-2002-07
PostNuke Development Team ¹⁷⁴⁴	Unix	PostNuke 0.721	PostNuke Cross-Site Scripting	High	CyberNotes-2002-20
PostNuke Development Team ¹⁷⁴⁵	Unix	PostNuke 0.721	PostNuke Remote SQL Injection	Low/ Medium (Medium if the database is corrupted)	CyberNotes-2002-20
Power boards ¹⁷⁴⁶	Multiple	Powerboards 2.2 b	Powerboards Multiple Vulnerabilities	Medium/High (High if administrative access can be obtained or if arbitrary code can be executed)	CyberNotes-2002-08
Power Phlogger ¹⁷⁴⁷	Unix	Power Phlogger 2.0.9, 2.2.1, 2.2.2 a	PowerPhlogger showhits.php3 Script	High	CyberNotes-2002-20
Powie ¹⁷⁴⁸	Unix	PForum 1.14	PForum User Authentication	High	CyberNotes-2002-04
Powie ¹⁷⁴⁹	Unix	PForum 1.11-1.14	Powie PForum Cross-Site Scripting	High	CyberNotes-2002-05
ProFTPD Project ¹⁷⁵⁰	Unix	ProFTPD 1.2.1- 1.2.6, 1.2.7rc3, 1.2.7 rc2, 1.2.7 rc1	ProFTPD STAT Command Denial of Service	Low	CyberNotes-2002-25
Progress ¹⁷⁵¹	Windows NT 4.0/2000, Unix	Database 9.1 B, 9.1 C	Progress sqlcpp Local Buffer Overflow	High	CyberNotes-2002-07
Progress ¹⁷⁵²	Windows NT 4.0/2000, Unix	Database 9.1 C	Progress _probrkr Buffer Overflow	High	CyberNotes-2002-09

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Prospero Technologies ¹⁷⁵³	Multiple	Message Boards	Message Board Cross-Site Scripting	High	CyberNotes-2002-04
Pserv ¹⁷⁵⁴	Multiple	Pserv 2.0 beta 1-beta 3	Pserv HTTP POST Request Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-24
Pserv ¹⁷⁵⁵	Unix	Pserv 2.0 beta1, beta2, beta3, beta5	Pserv Buffer Overflows	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-25
psyBNC ¹⁷⁵⁶	Unix	psyBNC 2.3	psyBNC Encrypted Conversation	Medium	CyberNotes-2002-02
psyBNC ¹⁷⁵⁷	Unix	psyBNC 2.3	psyBNC Denial of Service	Low	CyberNotes-2002-09
Punknews.org ¹⁷⁵⁸	Multiple	phpAnyVote 1.0	phpAnyVote Cookie Security Bypass	Medium	CyberNotes-2002-09
Purity ¹⁷⁵⁹	Unix	Purity 1-9, 1-14, 1-15	Purity Buffer Overflows	Medium	CyberNotes-2002-19
PVote ¹⁷⁶⁰	Multiple	PVote 1.0, 1.0.a, 1.0 b, 1.5	PVote Multiple Vulnerabilities	Medium	CyberNotes-2002-08
pWins ¹⁷⁶¹	Windows, Unix	pWins 0.2.5	pWins Directory Traversal	Medium	CyberNotes-2002-24
Py-Membres ¹⁷⁶²	Multiple	Py-Membres 3.1	Py-Membres Index.PHP Unauthorized Access	High	CyberNotes-2002-20
Pyramid ¹⁷⁶³	Multiple	BenHur Software Update 66	BenHur Default Firewall Ruleset	Medium	CyberNotes-2002-15
Python Software Foundation ¹⁷⁶⁴	Multiple	Python 1.5.2	Python Pickle Unsafe eval() Code Execution	High	CyberNotes-2002-15
Python Software Foundation ¹⁷⁶⁵	Multiple	Python 1.5.2, 1.6, 1.6.1, 2.0, 2.0.1, 2.1, 2.1.1, 2.1.2, 2.1.3	Python Pickle Class Constructor Arbitrary Code Execution	High	CyberNotes-2002-15
Python Software Foundation ¹⁷⁶⁶	Unix	Python 1.5.2, 1.6, 1.6.1, 2.0, 2.0.1, 2.1-2.1.3, 2.2, 2.2.1	Python 'os._execvpe' Predictable Temporary Filename	High	CyberNotes-2002-18
QNX Software Systems Ltd. ¹⁷⁶⁷	Multiple	QNX RTOS 4.25, 6.1.0	QNX RTOS Multiple Vulnerabilities	Medium/High (High if root access can be obtained or arbitrary code can be executed)	CyberNotes-2002-12
QNX Software Systems Ltd. ¹⁷⁶⁸	Multiple	RTOS 6.1.0	QNX RTOS PKG-Installer Buffer Overflow	High	CyberNotes-2002-12
QNX Software Systems Ltd. ¹⁷⁶⁹	Unix	Photon MicroGUI	QNX Photon MicroGUI Clipboard Insecure Data Storage	Medium	CyberNotes-2002-24
QNX Software Systems Ltd. ¹⁷⁷⁰	Unix	RTOS 6.2.0 Update Patch A, 6.2 .0	QNX Multiple Program Insecure Default Permissions	High	CyberNotes-2002-24
QNX Software Systems, Ltd. ¹⁷⁷¹	Multiple	RTOS 4.25	QNX RTOS Multiple Vulnerabilities	Medium/High (High if root access can be obtained)	CyberNotes-2002-12
QNX Software Systems, Ltd. ¹⁷⁷²	Multiple	RTOS 6.1.0	QNX Denial of Service	Low	CyberNotes-2002-23
QNX Software Systems, Ltd. ¹⁷⁷³	Multiple	RTOS 6.2	QNX RTOS Application Packager Non-Explicit Path Execution	High	CyberNotes-2002-23
Qualcomm Inc. ¹⁷⁷⁴	Windows 95/98/NT 4.0/2000	Eudora 5.1	Eudora Known Attachment Location	High	CyberNotes-2002-06
Qualcomm Inc. ¹⁷⁷⁵	Unix	QPopper 4.0-4.03	QPopper Remote Denial of Service	Low	CyberNotes-2002-06
Qualcomm Inc. ¹⁷⁷⁶	Windows 95/98/NT 4.0/2000	Eudora 5.1	Eudora WebBrowser Control Embedded Media Player File	High	CyberNotes-2002-07
Qualcomm Inc. ¹⁷⁷⁷	Unix	QPopper 4.0.3, 4.0.4	QPopper Bulletin Name Buffer Overflow	High	CyberNotes-2002-09
Qualcomm, Inc. ¹⁷⁷⁸	Windows 95/98/NT 4.0/2000	Eudora 5.0.2 -Jr2, 5.0.2, 5.1, 5.1.1	Eudora MIME Multipart Boundary Buffer Overflow	High	CyberNotes-2002-16

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Qualcomm, Inc. ¹⁷⁷⁹ <i>Upgrade released¹⁷⁸⁰</i>	Windows 95/98/NT 4.0/2000	Eudora 5.1	Eudora File Attachment Spoofing	Medium	CyberNotes-2002-16 CyberNotes-2002-23
Quantum ¹⁷⁸¹	Multiple	Snap Server 4100	Snap Server TCP Sequence Number and Denial of Service	Low/ Medium (Medium if an existing connection can be hijacked)	CyberNotes-2002-12
RadioBird Software ¹⁷⁸²	Multiple	WebServer 4 All 1.23, 4 All 1.27	WebServer Buffer Overflow and Directory Traversal CVE Names: CAN-2002-1212, CAN-2002-1213	Low/ Medium (Medium if sensitive information can be obtained)	CyberNotes-2002-21
RadioBird Software ¹⁷⁸³	Windows NT	WebServer 4 All 1.28	WebServer 4 All Buffer Overflow	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-22
Rational Software ¹⁷⁸⁴	Unix	ClearCase 2002.05, 4.1	ClearCase Portscan Denial of Service	Low	CyberNotes-2002-24
Raxnet ¹⁷⁸⁵ <i>Upgrades now available for the rrdtool 'graph' vulnerability¹⁷⁸⁶</i>	Multiple	Cacti 0.5, 0.6-0.6.8	Cacti Multiple Vulnerabilities	Medium High (High if arbitrary code is executed)	CyberNotes-2002-18 CyberNotes-2002-19
RCA ¹⁷⁸⁷	Multiple	Digital Cable Modem DCM225E, DCM225	Digital Cable Modem Remote Denial of Service & Sensitive Information	Low/ Medium (Medium if sensitive information is obtained)	CyberNotes-2002-07
Real Networks, Inc. ¹⁷⁸⁸	Windows 98/ME/NT 4.0/2000, XP	RealPlayer 8.0 Win32, 8.0 Unix	RealPlayer Media File Buffer Overflow	High	CyberNotes-2002-01
Real Networks, Inc. ¹⁷⁸⁹	Windows 95/98/NT 4.0/2000, Unix	RealPlayer 6.0 Win32, 6.0 Unix	RealPlayer Directory Traversal	Medium	CyberNotes-2002-05
Real Networks, Inc. ¹⁷⁹⁰	Windows 98/NT 4.0/2000, XP	RealPlayer 8.0 Win32	RealPlayer Denial of Service	Low	CyberNotes-2002-05
Real Networks, Inc. ¹⁷⁹¹	Windows 95/98/ME/NT 4.0/2000, XP	RealJuke box 2 for Windows 1.0.2 .379, 1.0.2 .340, RealJuke box 2 Plus for Windows 1.0.2 .379, 1.0.2 .340, RealOne Player Gold for Windows 6.0.10 .505	RealJukebox Buffer Overflow	High	CyberNotes-2002-15
Real Networks, Inc. ¹⁷⁹²	Windows 95/98/ME/NT 4.0/2000, XP	RealJuke box 2 for Windows 1.0.2 .379, 1.0.2 .340, RealJuke box 2 Plus for Windows 1.0.2 .379, 1.0.2 .340, RealOne Player Gold for Windows 6.0.10 .505	RealJukebox Predictable File Extraction	High	CyberNotes-2002-15
Real Networks, Inc. ¹⁷⁹³	Windows 95/98/NT 4.0/2000, XP	RealOne Player 2.0, G2, 6.0 Win32, 7.0 Win32, 8.0 Win32	RealOne Player Buffer Overflow Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-24
Real Networks, Inc. ¹⁷⁹⁴	Windows 95/98/ME/ NT 4.0/2000, XP	RealOne Player, 2.0, Player Gold for Windows 6.0.10 .505	Multiple Unspecified RealOne Player Buffer Overflow	High	CyberNotes-2002-25
Reality Scope ¹⁷⁹⁵	Windows NT 4.0/2000	MyLogin 2000 version 1.0.0	MyLogin SQL Injection	Medium	CyberNotes-2002-10
ReBB ¹⁷⁹⁶	Multiple	ReBB 1.0	ReBB Cross-Site Scripting	High	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
RedHat ¹⁷⁹⁷	Unix	DocBook-utils 0.6-13, 0.6.9-2, 1.54.13	DocBook Tools Default Stylesheet Arbitrary File Write CVE Name: CAN-2002-0169	Medium	CyberNotes-2002-09
RedHat ¹⁷⁹⁸	Unix	Stronghold 3.0	Stronghold "SWISH" Information Disclosure	Medium	CyberNotes-2002-11
RedHat ¹⁷⁹⁹	Unix	RHMask 1.0 -9	RHMask Local File Overwrite	Medium	CyberNotes-2002-12
RedHat¹⁸⁰⁰ <i>SCO releases patch¹⁸⁰¹</i>	Unix	RedHat PXE Server 0.1; HP Secure OS software for Linux 1.0	Red Hat PXE Server Denial of Service CVE Name: CAN-2002-0835	Low	CyberNotes-2002-18 CyberNotes-2002-23
Red-M Communications Ltd. ¹⁸⁰²	Multiple	1050AP LAN access point	Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities CVE Names: CAN-2002-0393, CAN-2002-0394, CAN-2002-0395, CAN-2002-0396, CAN-2002-0397, CAN-2002-0398	Low/ Medium (Medium if unauthorized access can be obtained)	CyberNotes-2002-12
Research Systems ¹⁸⁰³	Windows, Unix	ION Script 1.4	ION Script Remote File Disclosure	Medium	CyberNotes-2002-23
RhinoSoft ¹⁸⁰⁴	Multiple	Serv-U 3.0, 3.1, 4.0.0.4	Serv-U Denial of Service	Low	CyberNotes-2002-23
Rich Media Technologies ¹⁸⁰⁵	Multiple	JustAdd Commerce Real Time Processing 5.0, Standard 5.0	JustAdd Commerce Information Disclosure	Medium	CyberNotes-2002-05
Rich Media Technologies ¹⁸⁰⁶	Windows 98/ME/2000	JustAdd Commerce Standard 5.0	JustAdd Commerce Insufficient Validation Hidden Form Field	Medium	CyberNotes-2002-24
Richard Gooch ¹⁸⁰⁷	Unix	SimpleInit 2.0.2	SimpleInit Inherit File Descriptor	High	CyberNotes-2002-12
Rit Research Labs ¹⁸⁰⁸	Windows 95/98/ME/NT 4.0/2000, XP	The Bat! 1.53d	The Bat! Remote Denial of Service	Low	CyberNotes-2002-05
Rlaj ¹⁸⁰⁹	Unix	WhoIS 1.0	Rlaj WhoIS Remote Shell Command Execution	High	CyberNotes-2002-13
Rob Flynn ¹⁸¹⁰	Unix	Gaim 0.56, 0.57	Gaim World Readable File	Medium	CyberNotes-2002-10
Rob Flynn^{1811, 1812, 1813} <i>More vendor updates¹⁸¹⁴</i>	Unix	Gaim 0.56, 0.57	Gaim Jabber Plug-In Buffer Overflow CVE Name: CAN-2002-0384	High	CyberNotes-2002-16 CyberNotes-2002-18
Rob Flynn ^{1815, 1816, 1817}	Unix	Gaim 0.56-0.59	Gaim Manual Browser Command CVE Name: CAN-2002-0989	High	CyberNotes-2002-18
Rod Clark ¹⁸¹⁸	Unix	Sendform versions 1.4.4 & prior	Sendform.cgi Directory Traversal CVE Name: CAN-2002-0710	Medium	CyberNotes-2002-16
RSync ¹⁸¹⁹	Unix	RSync 2.4.1, 2.4.3, 2.4.4, 2.4.6, 2.5.0-2, 2.5.0-1, 2.5.1_1, 2.5.1, 2.5.2	RSync Supplementary Group Privilege CVE Name: CAN-2002-0080	Medium	CyberNotes-2002-06
RTFM ¹⁸²⁰	Unix	ssldump 0.9 b2, 0.9 b1	ssldump Buffer Overflow/ Underflow	High	CyberNotes-2002-19
Rudi Benkovic ¹⁸²¹	Unix	JAWmail 1.0 -rc1, 1.0, 1.0.1	JAWmail Cross-Site Scripting	High	CyberNotes-2002-20
Ruslan Communications ¹⁸²²	Multiple	<Body> Builder	Ruslan Communications <Body>Builder SQL Injection	High	CyberNotes-2002-12
Rusty Dragon ¹⁸²³	Unix	phpBB Advanced Quick Reply Hack 1.0.0, 1.1.0	PHPBB Advanced Quick Reply Hack Remote Code Injection	High	CyberNotes-2002-23
Sabre Inc. ¹⁸²⁴	Windows NT	Sabre Desktop Reservation Software 4.4 G	Sabre Desktop Reservation Software Denial of Service CVE Name: CAN-2002-1191	Low	CyberNotes-2002-21
Safe.pm ¹⁸²⁵	Windows, Unix	Safe.pm 2.0 7, 2.0 6	Safe.pm Access Bypass	Medium	CyberNotes-2002-23
SafeTP ¹⁸²⁶	Windows 2000, Unix	SafeTP Server 1.46	SafeTP Passive Mode Sensitive Information	Medium	CyberNotes-2002-20

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Samba ¹⁸²⁷	Multiple	Samba 2.2.4	Samba Improperly Terminated Struct Buffer Overflow	High	CyberNotes-2002-18
Samba ^{1828, 1829, 1830, 1831, 1832, 1833, 1834}	Unix	Samba 2.2.2-2.2.6	Samba Server Encrypted Password Buffer Overrun	High	CyberNotes-2002-24
Sambar Technologies ¹⁸³⁵	Windows 95/98/ME/NT 4.0/2000	Sambar Server 5.1	Sambar Server Denial of Service	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-02
Sambar Technologies ¹⁸³⁶	Windows 95/98/ME/NT 4.0/2000	Sambar Server 5.0 beta1-6, 5.1	Sambar Server Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-07
Sambar Technologies ¹⁸³⁷	Windows 95/98/ME/NT 4.0/2000	Sambar Server 5.1	Sambar Server Script Source Disclosure	Low Medium (Medium if sensitive information is obtained)	CyberNotes-2002-08
SAP ¹⁸³⁸	Windows 95/98/NT 4.0/2000	SAPgui 4.6 for Windows, 4.6A-4.6D for Windows	SAPgui Denial of Service	Low	CyberNotes-2002-03
SAP ¹⁸³⁹	Multiple	SAP R/3	SAP R/3 with Oracle Unauthorized Data Access	Medium	CyberNotes-2002-09
SAP ¹⁸⁴⁰	Unix	SAP DB 7.3 .00	SAP DB Insufficient Checks	High	CyberNotes-2002-25
Sapio Design Ltd. ¹⁸⁴¹	Windows 95/98/NT 4.0	WebReflex 1.53	WebReflex Directory Traversal	Medium	CyberNotes-2002-25
Sapporo Works ¹⁸⁴²	Windows 2000	Black JumboDog 2.6.4, 2.6.5	Black JumboDog Buffer Overflow	High	CyberNotes-2002-02
SAS Institute, Incorporated ¹⁸⁴³	Windows, OS/390, OS/2, Unix	SAS Base 8.0, 8.1	SASTCPD Buffer Overflow and Format String	High	CyberNotes-2002-03
SAS Institute, Incorporated ¹⁸⁴⁴	Multiple	SAS Base 8.0, Integration Technologies 8.0	'SASTCPD' and 'netencralg' Arbitrary Code Execution	High	CyberNotes-2002-03
Savant ¹⁸⁴⁵	Windows	Savant Webserver 3.1	Savant Webserver Multiple Vulnerabilities	Low/ Medium/High (Medium if sensitive information is obtained and High if arbitrary code is executed)	CyberNotes-2002-19
Savant ¹⁸⁴⁶	Windows	Savant Webserver 3.1 & prior	Savant Webserver Buffer Overflow CVE Name: CAN-2002-1120	High	CyberNotes-2002-19
Sawmill ¹⁸⁴⁷	Unix	Sawmill 6.2-6.2.14	Sawmill Admin Password Insecure Default Permissions	Medium	CyberNotes-2002-04
SCO ¹⁸⁴⁸	Unix	Open Server 5.0-5.0.6	OpenServer XSCO Heap Overflow	High	CyberNotes-2002-12
Scripts For Educators ¹⁸⁴⁹	Multiple	MakeBook 2.2	MakeBook Input Validation	High	CyberNotes-2002-12
Script-Shed ¹⁸⁵⁰	Multiple	SSGBook 1.0	SSGBook Image Tag	High	CyberNotes-2002-21
Seanox ¹⁸⁵¹	Windows	DevWex Windows Binary 1.2002.0520	DevWex Multiple Vulnerabilities	Low/ High (High if arbitrary code can be executed)	CyberNotes-2002-12
SEH ¹⁸⁵²	Multiple	IC9 7.1 .36, .30	SC9 Administrative Interface Password Denial Of Service	Low	CyberNotes-2002-16
Sendmail Consortium ¹⁸⁵³	Unix	Sendmail 8.9.0-8.9.3, 8.10-8.10.28.11-8.11.6 8.12, 8.12 beta5,7,10, 12, 16, 8.12.1- 8.12.3	Sendmail Denial Of Service	Low	CyberNotes-2002-11

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Sendmail Consortium ¹⁸⁵⁴	Unix	Sendmail 8.11- 8.11.6, 8.12- 8.12.4	Sendmail DNS Buffer Overflow	High	CyberNotes-2002-14
Sendmail Consortium ¹⁸⁵⁵	Unix	Sendmail 8.12 .0- 8.12.6	Sendmail Ident Logging Circumvention	Low	CyberNotes-2002-20
Sendmail Consortium ¹⁸⁵⁶	Unix	Sendmail 8.12.0- 8.12.6	Sendmail SMRSH Security Bypass CVE Name: CAN-2002-1165	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-20
Sendmail Consortium ¹⁸⁵⁷	Multiple	Sendmail 8.12.6	Sendmail Trojan Horse	Medium	CyberNotes-2002-21
Seunghyun Seo ¹⁸⁵⁸	Multiple	MSN666 1.0, 1.0.1	MSN666 Remote Buffer Overflow	High	CyberNotes-2002-13
SGI ¹⁸⁵⁹	Unix	IRIX 6.4, 6.5, 6.5.1, 6.5.2m, 6.5.2f, 6.5.2, 6.5.3m, 6.5.3f, 6.5.3, 6.5.4m/f-6.5.11m/f	IRIX nsd Denial of Service CVE Name: CAN-2002-0038	Low	CyberNotes-2002-02
SGI ¹⁸⁶⁰	Unix	IRIX 6.5.10m, 6.5.10f, 6.5.11, 6.5.11f, 6.5.11m, 6.5.12, 6.5.12f, 6.5.12m, 6.5.13, 6.5.13f, 6.5.13m, 6.5.14, 6.5.14f, 6.5.14m	IRIX Output Video Viewing	Medium	CyberNotes-2002-03
SGI ¹⁸⁶¹	Unix	IRIX 6.5, 6.5.1, 6.5.2-6.5.14, 6.5.2m- 6.5.14m, 6.5.2f- 6.5.14f, 6.5.15m, 6.5.15f	IRIX SNMP Daemon Buffer Overflow CVE Name: CAN-2002-0013, CAN-2002-0017	High	CyberNotes-2002-07
SGI ¹⁸⁶²	Unix	IRIX 6.5-6.5.10, 6.5.11m- 6.5.15m, 6.5.11f- 6.5.15f	SGI IRIX Denial of Service Vulnerabilities CVE Names: CAN-2002-0039, CAN-2002-0040	Low	CyberNotes-2002-07
SGI ¹⁸⁶³	Unix	IRIX 6.5-6.5.10, 6.5.11m- 6.5.15m, 6.5.11f- 6.5.15f	SGI IRIX Mail Vulnerabilities	Medium	CyberNotes-2002-08
SGI ¹⁸⁶⁴	Unix	IRIX 6.5-6.5.9, 6.5.10&11m 6.5.10&11f	IRIX XFS Filesystem Denial of Service CVE Name: CAN-2002-0042	Low	CyberNotes-2002-08
SGI ¹⁸⁶⁵	Unix	IRISconsole 2.0	IRISconsole icadmin Unauthorized Access CVE Name: CAN-2002-0171	Medium	CyberNotes-2002-09
SGI ¹⁸⁶⁶	Unix	IRIX 5.0-5.3, 6.0- 6.5.10, 6.5.2 m-6.5.10 m, 6.5.2 f- 6.5.10 f	Irix CPR Buffer Overflow CVE Name: CAN-2002-0173	High	CyberNotes-2002-09
SGI ¹⁸⁶⁷	Unix	IRIX 6.5, 6.5.1-6.5.9	Irix syslogd Remote Denial of Service CVE Names: CAN-1999-0171, CVE-1999-0566	Low	CyberNotes-2002-09
SGI ¹⁸⁶⁸	Unix	IRIX 6.5-6.5.10	Irix Performance Co-Pilot Remote Denial of Service CVE Name: CAN-2000-1193	Low	CyberNotes-2002-09
SGI ¹⁸⁶⁹	Unix	IRIX 6.5-6.5.10	Irix Insecure IPFilter Device Permissions CVE Name: CAN-2002-0172	Low/ Medium (Medium if unauthorized access is obtained)	CyberNotes-2002-09
SGI ¹⁸⁷⁰	Unix	IRIX 6.5-6.5.10	Irix NSD Symbolic Link CVE Name: CAN-2002-0174	Medium	CyberNotes-2002-09

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
SGI ¹⁸⁷¹	Unix	snmpd.sw.hp 1.1.2, 1.1.3	Irix hpsnmpd Denial of Service CVE Names: CAN-2002-0012, CAN-2002-0013	Low	CyberNotes-2002-09
SGI ¹⁸⁷²	Unix	IRIX 6.5-6.5.10, 6.5f-6.5.10f, 6.5m- 6.5.10m	SGI IRIX fsr_xfs Root Access CVE Name: CAN-2002-0356	High	CyberNotes-2002-10
SGI ¹⁸⁷³	Unix	IRIX 6.5-6.5.11	IRIX 'netstat' Sensitive Information CVE Name: CAN-2002-0355	Medium	CyberNotes-2002-10
SGI ¹⁸⁷⁴	Unix	IRIX 5.0-5.3, 6.0-6.5.16	IRIX MediaMail Memory Corruption CVE Name: CAN-2002-0358	Medium	CyberNotes-2002-12
SGI ¹⁸⁷⁵	Unix	IRIX 6.5-6.5.15, 6.5.2f- 6.5.15f, 6.5.2m- 6.5.15m	IRIX rpc.passwd Buffer Overflow CVE Name: CAN-2002-0357	High	CyberNotes-2002-12
SGI ¹⁸⁷⁶	Unix	IRIX 6.2-6.5, 6.5.1- 6.5.16, 6.5.1f- 6.5.15f, 6.5.1m- 6.5.15m	IRIX rpc.xfsmd Remote Command Execution & Weak Authentication CVE Name: CAN-2002-0359	High	CyberNotes-2002-13
SGI ¹⁸⁷⁷	Unix	IRIX 6.5- 6.5.16	SGI NetVisualyzer Arbitrary File Write CVE Name: CAN-2002-0631	Medium/ High (High if root access can be obtained)	CyberNotes-2002-13
SGI ¹⁸⁷⁸	Unix	IRIX 6.5.13- 6.5.16	IRIX MAC Address Changing	Medium	CyberNotes-2002-17
SGI ¹⁸⁷⁹	Unix	IRIX 6.5-6.5.16	SGI Irix Bulk Data Services Arbitrary File Disclosure CVE Name: CAN-2002-0632	Medium	CyberNotes-2002-17
SGI ¹⁸⁸⁰	Unix	IRIX 6.5-6.5.16	IRIX ftpd PASV Mode Hijacking	Medium	CyberNotes-2002-17
SGI ¹⁸⁸¹	Unix	IRIX 6.5-6.5.14	IRIX Coredump Umask	Medium	CyberNotes-2002-19
SGI ¹⁸⁸²	Unix	IRIX 6.5-6.5.17, 6.5.13 m- 6.5.17m	IRIX Multiple Vulnerabilities	Low/ Medium/High Low if a Denial of Service; Medium if files are overwritten or elevated privileges obtained; and High if arbitrary code can be executed)	CyberNotes-2002-21
SH39 ¹⁸⁸³	Windows 2000	MailServer 1.2.1	MailServer Denial of Service	Low	CyberNotes-2002-05
Shana Corporation ¹⁸⁸⁴	Windows, MacOS, Unix	Informed Designer 3.5, Informed Filler 3.5	Shana Informed Information Disclosure	Medium	CyberNotes-2002-20
Sharman Networks ¹⁸⁸⁵	Windows 95/98/ME/NT 4.0/2000, XP	KaZaA Media Desktop 1.7.1	KaZaA Media Desktop Denial of Service	Low	CyberNotes-2002-15
Sharp Electronics ¹⁸⁸⁶	Unix	Zaurus SL-5000D, SL-5500	Zaurus Multiple Vulnerabilities	Medium/High (High if root access is obtained)	CyberNotes-2002-14
Siemens ¹⁸⁸⁷	Multiple	3568i WAP	Siemens Mobile Phone Denial of Service	Low	CyberNotes-2002-02
Simple WAIS ¹⁸⁸⁸	Unix	Simple WAIS 1.11	Simple WAIS Interface Arbitrary Command Execution	High	CyberNotes-2002-14
Sitenews ¹⁸⁸⁹	Windows NT 4.0/2000, Unix	Sitenews 0.01 beta- 0.11 beta	Sitenews Unauthorized Control	High	CyberNotes-2002-04
Sky Stream Networks ¹⁸⁹⁰	Unix	EMR5000 1.16, 1.17, 1.18	Edge Media Remote Denial of Service	Low	CyberNotes-2002-21

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
SlashCode ¹⁸⁹¹	Unix	SlashCode 2.1-2.2.2	SlashCode Administrative Account	High	CyberNotes-2002-02
SlashCode ¹⁸⁹²	Unix	SlashCode 1.0.8 and previous, 2.0-2.2.4	SlashCode Cross-Site Scripting	High	CyberNotes-2002-04
SLRN Development Team ¹⁸⁹³	Unix	SLRN 0.9.6 .2 - 0.9.6.4	SLRNPull Spool Directory Buffer Overflow	High	CyberNotes-2002-09
SmartMax ¹⁸⁹⁴	Multiple	Software MailMax 4.8	MailMax Popmax Buffer Overflow	High	CyberNotes-2002-15
SMB2 WWW ¹⁸⁹⁵	Unix	SMB2 WWW 980804, 980802, 980727, 980427	SMB2WWW Remote Command Execution	High	CyberNotes-2002-25
Snapgear ¹⁸⁹⁶	Multiple	Lite+ Firewall 1.5.3, 1.5.4	Lite+ Firewall Denial of Service Vulnerabilities	Low/High (High if DDoS best practices not in place)	CyberNotes-2002-09
Sniffit ¹⁸⁹⁷	Unix	Sniffit 0.3.7beta	Sniffit Mail Buffer Overflow	High	CyberNotes-2002-02
Snitz Forums 2000 ¹⁸⁹⁸	Windows	Snitz Forums 2000 3.0, 3.1, 3.3.01-3.3.03, 3.3	Snitz Forums 2000 Cross-Site Scripting	High	CyberNotes-2002-05
Snitz Forums 2000 ¹⁸⁹⁹	Windows	Snitz Forums 2000 3.0, 3.1, 3.3.01-3.3.03, 3.3	Snitz Forums 2000 Members.ASP SQL Injection	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-09
Snort Center ¹⁹⁰⁰	Unix	Snort Center 0.9.5	SnortCenter Temporary File Access & Insecure Configuration Permissions	Medium	CyberNotes-2002-23
Software 602 ¹⁹⁰¹	Windows 98/ME/NT 4.0/2000, XP	602Pro LAN SUITE 2002	Web602 Unauthorized Admin Directory Access	High	CyberNotes-2002-22
Solar Winds ¹⁹⁰²	Windows	TFTP Server Standard Edition 5.0.55	TFTP Server Large UDP Packet Denial of Service	Low	CyberNotes-2002-22
Solar Winds ¹⁹⁰³	Windows	TFTP Server Standard Edition 5.0.55	TFTP Server Directory Traversal	Medium	CyberNotes-2002-22
Sonic WALL ¹⁹⁰⁴	Multiple	SOHO 6.3.0.0	SOHO Content Blocking Script Injection	High	CyberNotes-2002-11
Sonic WALL ¹⁹⁰⁵	Multiple	Content Filtering	Content Filtering Software Bypassing	Medium	CyberNotes-2002-22
Sony ¹⁹⁰⁶	Multiple	VAIO Manual for UAE, Southeast Asia, South Africa, Saudi Arabia, Oceania, East Asia, Manual Cyber Support for VAIO 3.0&3.1 Japan	VAIO Unauthorized Access	High	CyberNotes-2002-03
Sourcecraft ¹⁹⁰⁷	Windows, Unix	Networking_Utills 1.0	Networking_Utills Input Validation	High	CyberNotes-2002-23
SouthWest ¹⁹⁰⁸	Windows 95/98/NT 4.0	SouthWest 1.0 .0	SouthWest Denial of Service	Low	CyberNotes-2002-07
Splatt.it ¹⁹⁰⁹	Multiple	Splatt Forum 3.0	Splatt Forum Image Tag HTML Injection	High	CyberNotes-2002-12
SQLData Systems ¹⁹¹⁰	Windows 95/NT 4.0	SQLData Enterprise Server 3.0	SQLData Enterprise Server Buffer Overflow	High	CyberNotes-2002-01
Squirrel Mail ¹⁹¹¹	Unix	SquirrelMail 1.2.2	SquirrelMail 'compose.php' Script	High	CyberNotes-2002-02
Squirrel Mail ¹⁹¹²	Unix	SquirrelSpell 0.3.5	SquirrelSpell Plugin	High	CyberNotes-2002-02
Squirrel Mail ¹⁹¹³	Unix	SquirrelMail 1.2.5	SquirrelMail Theme Remote Command Execution	High	CyberNotes-2002-07
Squirrel Mail ¹⁹¹⁴	Unix	SquirrelMail 1.2 .0-1.2.5	SquirrelMail HTML Attachment Script Injection	High	CyberNotes-2002-10
Squirrel Mail ¹⁹¹⁵	Unix	Squirrel Mail 1.2.9	SquirrelMail Cross-Site Scripting	High	CyberNotes-2002-25
SquirrelMail ¹⁹¹⁶ <i>RedHat issues updated advisory¹⁹¹⁷</i> <i>Debian issues advisory¹⁹¹⁸</i>	Unix	SquirrelMail 1.2.7	SquirrelMail Multiple Cross-Site Scripting CVE Name: CAN-2002-1131	High	CyberNotes-2002-19 CyberNotes-2002-21 CyberNotes-2002-23

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
SquirrelMail ¹⁹¹⁹ <i>Debian issues advisory</i> ¹⁹²⁰	Unix	SquirrelMail 1.2.7	SquirrelMail Options.PHP CVE Name: CAN-2002-1132	Medium	CyberNotes-2002-21 CyberNotes-2002-23
SSH Communications Security ¹⁹²¹	Unix	SSH for UNIX 1.2.33, SSH2 3.0, 3.0.1	SSH Restricted Shell Escaping Command Execution	Medium	CyberNotes-2002-08
SSH Communications Security ¹⁹²²	Windows, Unix	SSH2 3.0, 3.0.1, SSH2 for Unix 3.1, 3.1.1, SSH2 for Win32 3.1, 3.1.1	SSH2 Authentication Bypass	Medium	CyberNotes-2002-11
SSH Communications Security ¹⁹²³	Unix	SSH2 2.0.13, 2.1-2.5, 3.0, 3.0.1, 3.1- 3.1.4, 3.2, 3.2.1	SSH Server Privilege Escalation	Medium	CyberNotes-2002-24
SSH Communications Security ¹⁹²⁴	Windows	SSH2 3.1, 3.1.1-3.1.4, 3.2	Secure Shell Windows Client URL Buffer Overflow	High	CyberNotes-2002-24
Stefan Holmberg ¹⁹²⁵	Multiple	AdMentor 2.11	AdMentor Remote Login	High	CyberNotes-2002-04
Stellar-X Software ¹⁹²⁶	Windows NT	MSNTAuth 2.0	Stellar-X Format String	High	CyberNotes-2002-12
Stephen Ball ¹⁹²⁷	Multiple	File Manager 1.5	File Manager Directory Traversal & Privilege Elevation	Medium	CyberNotes-2002-17
Stephen Hebditch ¹⁹²⁸	Unix	slurp 1.10	Slurp Remote Format String	High	CyberNotes-2002-12
StepWeb ¹⁹²⁹	Unix	SWS 2.5	StepWeb Search Engine Administrative Access	High	CyberNotes-2002-08
Steve Kneizys ¹⁹³⁰	Multiple	Agora.cgi 3.2-3.2r, 3.3a-3.3f, 3.3i, 3.3j, 4.0-4.0e	Agora.CGI Path Disclosure	Medium	CyberNotes-2002-03
STunnel ^{1931, 1932}	Unix	STunnel 3.15-3.21c	STunnel Client Negotiation Protocol Format String CVE Name: CAN-2002-0002	High	CyberNotes-2002-01
Sublimation.org ¹⁹³³	Unix	SCPOOnly 2.3, 2.4	SCPOOnly SSH Environment Shell Escaping	High	CyberNotes-2002-17
Summit Computer Networks ¹⁹³⁴	Windows NT 4.0/2000	Lil'HTTP 2.1	Lil' HTTP Web Server Sensitive Information	Medium	CyberNotes-2002-05
Summit Computer Networks ¹⁹³⁵	Windows NT 4.0/2000	Lil'HTTP 2.1, 2.2	Lil' HTTP Server Directory Traversal	Medium	CyberNotes-2002-09
Summit Computer Networks ¹⁹³⁶	Windows NT 4.0/2000	Lil'HTTP 2.1, 2.2	Lil' HTTP Server Cross-Site Scripting	High	CyberNotes-2002-13
Summit Computer Networks ¹⁹³⁷	Windows NT 4.0/2000	Lil'HTTP 2.1, 2.2	Lil' HTTP 'pbcgi.cgi' Cross-Site Scripting	High	CyberNotes-2002-15
Sun Microsystems, Inc. ¹⁹³⁸	Unix	Sun SMC 2.0	Sun SMCBoot Insecure Temporary File Creation Directory Destruction	Medium	CyberNotes-2002-01
Sun Microsystems, Inc. ¹⁹³⁹	Unix	JRE (Linux Production Release) 1.2.2, 1.3.1	JRE Denial of Service	Low	CyberNotes-2002-03
Sun Microsystems, Inc. ¹⁹⁴⁰	Unix	Solaris 2.5.1, 2.5.1_x86& ppc, 2.6sparc, 2.6HW5/98, 2.6HW3/98, 2.6_x86HW5/98, 2.6_x86HW3/98, 2.6_x86, 2.6, 7.0_x86, 7.0_x86, 0, 8.0_x86, 8.0	Solaris Mail Command Execution	High	CyberNotes-2002-04
Sun Microsystems, Inc. ¹⁹⁴¹	Unix	Cobalt RaQ 2.0-4.0	Cobalt RaQ Multiple Vulnerabilities	Low/ Medium/High (Medium for the Directory Traversal Vulnerability and High if arbitrary code can be executed)	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Sun Microsystems, Inc. ¹⁹⁴²	Windows, Unix	Windows Production Releases SDK & JRE 1.3.0_02 or earlier, SDK & JRE 1.2.2_010 or earlier, JDK & JRE 1.1.8_007 or earlier, Solaris Operating Environment Reference Releases SDK & JRE 1.2.2_010 or earlier, JDK & JRE 1.1.8_007 or earlier, Solaris Production Releases SDK & JRE 1.3.0_02 or earlier, SDK & JRE 1.2.2_10 or earlier, JDK & JRE 1.1.8_13 or earlier, Linux Production Releases SDK & JRE 1.3.0_02 or earlier, SDK & JRE 1.2.2_010 or earlier	Sun Java Applet Browser Traffic Redirect CVE Name: CAN-2002-0058	High	CyberNotes-2002-05
Sun Microsystems, Inc. ¹⁹⁴³	Unix	Cobalt RaQ 2.0-4.0	Cobalt RaQ MultiFile Upload.php Authentication Bypass	High	CyberNotes-2002-06
Sun Microsystems, Inc. ¹⁹⁴⁴	Unix	Solaris 7.0, 7.0_x86, 8.0, 8.0_x86	Sunsolve CD CGI Script	High	CyberNotes-2002-06
Sun Microsystems, Inc. ¹⁹⁴⁵	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris XSun Buffer Overflow CVE Name: CAN-2002-0158	High	CyberNotes-2002-07
Sun Microsystems, Inc. ¹⁹⁴⁶	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris cachefsd Denial of Service CVE Name: CAN-2002-0085	Low	CyberNotes-2002-09
Sun Microsystems, Inc. ¹⁹⁴⁷	Unix	Solaris 2.6, 7.0, 8.0	Solaris AdminTool Buffer Overflow CVE Name: CAN-2002-0088	High	CyberNotes-2002-09
Sun Microsystems, Inc. ¹⁹⁴⁸	Unix	Solaris 8.0, 8.0_x86	Solaris LBXProxy Buffer Overflow CVE Name: CAN-2002-0090	High	CyberNotes-2002-09
Sun Microsystems, Inc. ¹⁹⁴⁹	Unix	Solaris2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris cachefsd Buffer Overflow CVE Name: CAN-2002-0084	High	CyberNotes-2002-09
Sun Microsystems, Inc. ¹⁹⁵⁰	Unix	Sun Solaris 2.5, 2.5_x86, 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris Local Buffer Overflows CVE Name: CAN-2002-0089	High	CyberNotes-2002-09
Sun Microsystems, Inc. ¹⁹⁵¹	Unix	Sun Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Sun Solaris RWall Daemon Syslog Format String	High	CyberNotes-2002-09
Sun Microsystems, Inc. ¹⁹⁵²	Unix	Sun Solaris 2.5.1, 2.5.1_x86, _ppc, 2.6, 2.6_sparc, _x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris cachefsd Buffer Overflow CVE Name: CAN-2002-11	High	CyberNotes-2002-10
Sun Microsystems, Inc. ¹⁹⁵³	Unix	SunATM 4.0 Update 1, 5.0	SunATM Agent SNMP Request Handling	Low	CyberNotes-2002-10
Sun Microsystems, Inc. ¹⁹⁵⁴	Unix	Answer Book2 1.4-1.4.3	AnswerBook2 Gettransbitmap Buffer Overflow CVE Name: CAN-2002-0360	High	CyberNotes-2002-11
Sun Microsystems, Inc. ¹⁹⁵⁵	Unix	in.rarpd	Solaris In.Rarpd Multiple Vulnerabilities	High	CyberNotes-2002-11
Sun Microsystems, Inc. ¹⁹⁵⁶	Unix	Solaris 9ea & prior	Solaris in.talkd Remote Root Compromise	High	CyberNotes-2002-11
Sun Microsystems, Inc. ¹⁹⁵⁷	Unix	Sun Solaris 2.6_x86, 2.6, 7.0_x86, 7.0, 8.0_x86, 8.0	Sun Solaris snmpdx Format String & mibiisa Remote Buffer Overflow	High	CyberNotes-2002-12
Sun Microsystems, Inc. ¹⁹⁵⁸	Unix	Solaris 8.0, 8.0_x86	Solaris Screensaver Authentication Bypass	Medium	CyberNotes-2002-13
Sun Microsystems, Inc. ¹⁹⁵⁹	Unix	Solaris 9.0	Sun Solaris RCP Command Line Argument Buffer Overflow	Medium	CyberNotes-2002-13

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Sun Microsystems, Inc. ¹⁹⁶⁰	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86	Solaris Serial Console Keystroke Interception	Medium	CyberNotes-2002-14
Sun Microsystems, Inc. ¹⁹⁶¹	Unix	Solaris 2.5.1, 2.6, 7.0, 8.0	Sun Solaris pkgadd Inappropriate File Permissions	High	CyberNotes-2002-14
Sun Microsystems, Inc. ¹⁹⁶²	Unix	Solaris 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris 7/8 KCMS Buffer Overflow	High	CyberNotes-2002-14
Sun Microsystems, Inc. ¹⁹⁶³	Unix	Solaris 8.0, 8.0_x86	Solaris /dev/poll Denial of Service	Low	CyberNotes-2002-14
Sun Microsystems, Inc. ¹⁹⁶⁴	Unix	SunPCi II Driver Software 2.3	SunPCi II Weak Authentication Scheme	Medium	CyberNotes-2002-14
Sun Microsystems, Inc. ¹⁹⁶⁵	Unix	i-Runbook 2.5.2	i-Runbook Directory And File Content Disclosure	Medium	CyberNotes-2002-15
Sun Microsystems, Inc. ¹⁹⁶⁶	Unix	Java Web Start 1.0, 1.0.1, 1.0.1_01, 1.0.1_02	Java Web Start JNLP Predictable File Location	High	CyberNotes-2002-15
Sun Microsystems, Inc. ¹⁹⁶⁷	Windows	PC NetLink 1.0, 1.1, 1.2	PC NetLink Backup Restoration ACL Permissions	Medium	CyberNotes-2002-15
Sun Microsystems, Inc. ¹⁹⁶⁸	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris Volume Manager Buffer Overflow	High	CyberNotes-2002-15
Sun Microsystems, Inc. ¹⁹⁶⁹	Unix	Sun Fire 280R, V480, V880	Sun Fire Denial of Service	Low	CyberNotes-2002-15
Sun Microsystems, Inc. ¹⁹⁷⁰	Unix	Answer Book2 1.2, 1.3.x, 1.4-1.4.2	AnswerBook2 Unauthorized Administrative Script Access	High	CyberNotes-2002-16
Sun Microsystems, Inc. ¹⁹⁷¹	Unix	Solaris 2.5.1, 2.6, 2.6_sparc, 7.0, 8.0	Solaris GFXRES / PGXConfig Buffer Overflow	High	CyberNotes-2002-16
Sun Microsystems, Inc. ¹⁹⁷²	Multiple	Cobalt RaQ 4.0	Cobalt RaQ Elevated Privileges	Medium	CyberNotes-2002-17
Sun Microsystems, Inc. ¹⁹⁷³	Unix	PatchPro 2.0	PatchPro Insecure Temporary File	Medium	CyberNotes-2002-17
Sun Microsystems, Inc. ¹⁹⁷⁴	Unix	Solaris 2.4, 2.5, 2.5.1_x86, 2.5.1, 2.6_x86, 2.6, 7.0_x86, 7.0, 8.0_x86, 8.0	Sun XView Buffer Overflow	High	CyberNotes-2002-17
Sun Microsystems, Inc. ¹⁹⁷⁵	Unix	7.0, 7.0_x86, 8.0, 8.0_x86	CDE ToolTalk Set Default Session Core Dump	Medium	CyberNotes-2002-18
Sun Microsystems, Inc. ¹⁹⁷⁶	Unix	Cobalt Control Station 4100CS, Cobalt Qube3 4000WG, Qube3 w/ Caching & RAID 4100WG, Qube3 w/Caching 4010WG, RaQ XTR 3500R, RaQ4 3001R, RaQ4 RAID 3100R	RaQ authenticate Root Privilege Escalation	High	CyberNotes-2002-19 CyberNotes-2002-24
<i>Upgrade now available and exploit script published¹⁹⁷⁷</i>					
Sun Microsystems, Inc. ¹⁹⁷⁸	Unix	Solaris 8.0, 8.0_x86	Sun Solaris ASPPPLS Insecure Temporary File Creation	High	CyberNotes-2002-19
Sun Microsystems, Inc. ¹⁹⁷⁹	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Sun Solaris TTYPROMPT Authentication Bypass	Medium/High (High if root access can be obtained)	CyberNotes-2002-20
Sun Microsystems, Inc. ¹⁹⁸⁰	Unix	Solaris 2.5, 2.5.1, 2.5.1_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	Solaris NFS lockd Remote Denial of Service	Low	CyberNotes-2002-21
Sun Microsystems, Inc. ¹⁹⁸¹	Unix	Solaris 8.0_x86, 8.0	Sun Solaris 8 KMEM_FLAG Denial of Service	Low	CyberNotes-2002-22
Sun Microsystems, Inc. ¹⁹⁸²	Unix	Solaris 8.0, 8.0_x86	Sun Solaris WBEM Insecure Permissions	Low/ Medium (Medium if sensitive information can be obtained or elevated privileges can be obtained)	CyberNotes-2002-22
Sun Microsystems, Inc. ¹⁹⁸³	Unix	Solaris 8.0, 8.0_x86, 9.0	Sun Solaris Local/Remote Denial of Service	Low	CyberNotes-2002-23
Sun Microsystems, Inc. ¹⁹⁸⁴	Windows NT 4.0/2000, Unix	iPlanet Web Server 4.1, 4.1 SP1-SP11	iPlanet Admin Cross-Site Scripting & Unsafe Perl Script open() Calls	High	CyberNotes-2002-24

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Sun Microsystems, Inc. ¹⁹⁸⁵	Unix	Solaris 2.5.1, 2.6, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	Solaris priocntl() System Call Local Root	Medium	CyberNotes-2002-24
Sun Microsystems, Inc. ¹⁹⁸⁶	Multiple	Cobalt RaQ 4.0	Cobalt RaQ4 Administrative Interface Command Execution	High	CyberNotes-2002-25
Sun Microsystems, Inc. ¹⁹⁸⁷	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris Libthread Library Denial of Service	Low	CyberNotes-2002-25
Sun Microsystems, Inc. ¹⁹⁸⁸	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	Solaris Denial of Service	Low	CyberNotes-2002-25
Sun Microsystems, Inc. ¹⁹⁸⁹	Unix	Solaris 26, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Solaris MailTool Attachment Denial of Service	Low	CyberNotes-2002-25
Sun Microsystems, Inc. / Astaware Technologies Inc. ¹⁹⁹⁰	Unix	Sun ONE Starter Kit 2.0; ASTAware SearchDisc 3.1	Sun ONE Starter Kit / ASTAware SearchDisc Search Engine Directory Traversal	Medium	CyberNotes-2002-20
Sun Microsystems, Inc. / iPlanet ¹⁹⁹¹	Windows NT 4.0/2000, Unix	Sun ONE Web Server 4.1, 6.0; iPlanet E-Commerce Solutions iPlanet Web Server 4.x, 4.1, 4.1 SP1-9, 6.0, 6.0 SP1&2	Sun ONE/iPlanet Web Server Chunked Encoding	High	CyberNotes-2002-16
Sun/ Netscape ¹⁹⁹² <i>Sun releases upgrade¹⁹⁹³</i>	Windows, Unix	Netscape Communicator 4.0-4.8; Sun Java 2 Runtime Environment 1.1-1.4	Sun/Netscape Java Virtual Machine Bytecode Verifier	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-24 CyberNotes-2002-25
Surecom ¹⁹⁹⁴	Multiple	EP-4501	EP-4501 Router SNMP Default Community Strings	Low/ Medium (Medium if sensitive information can be obtained)	CyberNotes-2002-23
Surf Control ¹⁹⁹⁵	Windows NT 4.0/2000	SuperScout Web Filter for Windows NT/2000 3.0, 3.0.3, 4.0, 4.1	SuperScout Multiple Vulnerabilities CVE Names: CAN-2002-0705, CAN-2002-0706, CAN-2002-0707, CAN-2002-0708, CAN-2002-0709	Low/ Medium (Medium if sensitive information is obtained)	CyberNotes-2002-20
Surf Control ¹⁹⁹⁶	Windows NT 4.0/2000	SuperScout E-mail Filter 3.5, 3.5.1, SuperScout E-mail Filter for SMTP 4.0	SuperScout E-mail Filter Multiple Vulnerabilities	Low/ Medium/High Low for the Denial of Service, Medium if sensitive information can be obtained, and High if arbitrary code can be executed)	CyberNotes-2002-21
SurfControl ¹⁹⁹⁷	Windows NT 4.0/2000	SuperScout Email Filter SMTP 3.5.1	SurfControl Denial of Service	Low	CyberNotes-2002-06
SuSE ¹⁹⁹⁸	Unix	Linux 8.0	Shadow File Truncation	Medium	CyberNotes-2002-10
SuSE ¹⁹⁹⁹	Unix	Linux 8.0 i386	SuSE IfUp-DHCP Script Remote Arbitrary Command Execution	High	CyberNotes-2002-10
SuSE ²⁰⁰⁰	Unix	XFree86 X11R6 4.2.0	XFree86 libX11.so Local Privilege Escalation	High	CyberNotes-2002-19

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
SuSE ²⁰⁰¹ <i>Debian issues advisory²⁰⁰²</i> <i>Exploit script has been published²⁰⁰³</i> <i>Debian updates advisory²⁰⁰⁴</i>	Unix	Linux 7.0-7.3, 8.0, 8.1	LPRNG Runlpr & html2ps Command Execution	High	CyberNotes-2002-22 CyberNotes-2002-23 CyberNotes-2002-24 CyberNotes-2002-25
SWS ²⁰⁰⁵	Multiple	Simple Web Server 0.0.4, 0.0.3, 0.1.1, 0.1.0	SWS Simple Web Server Non-existent File Request Denial Of Service	Low/ Medium (Medium if sensitive information is obtained)	CyberNotes-2002-18
SWS ²⁰⁰⁶	Unix	Simple Web Server 0.0.4, 0.0.3, 0.1.0	Simple Web Server Remote Denial of Service	Low	CyberNotes-2002-19
Sybase ²⁰⁰⁷	Windows NT 4.0, Unix	Adaptive Server Enterprise 12.0 Win, 12.0 Sun, 12.0 HP, 12.5 Win, 12.5 Sun, 12.5 HP, 12.5 SGI, 12.5 Digital UNIX	Adaptive Server DBCC CHECK VERIFY Buffer Overflow	High	CyberNotes-2002-24
Sybase ²⁰⁰⁸	Windows NT 4.0, Unix	Adaptive Server Enterprise 12.0 Win, 12.0 Sun, 12.0 HP, 12.5 Win, 12.5 Sun, 12.5 HP, 12.5 SGI, 12.5 Digital UNIX	Adaptive Server DROP DATABASE Buffer Overflow	High	CyberNotes-2002-24
Sybase ²⁰⁰⁹	Windows NT 4.0	Adaptive Server Enterprise 12.0 Win, 12.5 Win	Adaptive Server xp_freedll Buffer Overflow	High	CyberNotes-2002-24
Sybex ²⁰¹⁰	Windows 94/98/NT 4.0/2000	E-Trainer	E-Trainer Directory Traversal	Medium	CyberNotes-2002-04
Symantec ²⁰¹¹	Windows NT 4.0/2000	Enterprise Firewall 6.5.2 NT/2000	Enterprise Firewall SMTP Proxy Information Leak and Firewall Notify Daemon SNMP Data Loss	Medium	CyberNotes-2002-04
Symantec ²⁰¹²	Windows 98/NT 4.0/2000, XP	Ghost Corporate Edition 7.0	Ghost Corporate Edition Plaintext Account Information	Medium	CyberNotes-2002-05
Symantec ²⁰¹³	Multiple	LiveUpdate 1.4-1.7	LiveUpdate Plaintext Authentication	Medium	CyberNotes-2002-05
Symantec ²⁰¹⁴	Windows 98/ME/NT 4.0/2000, XP	Norton AntiVirus 2002 0.0	Symantec Norton AntiVirus Multiple Vulnerabilities	Medium	CyberNotes-2002-05
Symantec ²⁰¹⁵	Unix	Enterprise Firewall 7.0 Solaris, Raptor Firewall 6.5.3 Solaris	Raptor / Enterprise Firewall for Solaris FTP Bounce	Medium	CyberNotes-2002-08
Symantec ²⁰¹⁶	Multiple	Norton Personal Firewall 2002	Norton Personal Firewall 2002 Portscan Protection Bypass	Medium	CyberNotes-2002-08
Symantec ²⁰¹⁷	Multiple	Norton Personal Firewall 2002	Norton Personal Firewall 2002 Denial of Service	Low/High (High if DDoS best practices not in place)	CyberNotes-2002-08
Symantec ²⁰¹⁸	Windows 95/98/ME/NT 4.0/2000, XP	Norton Internet Security 2001, Norton Personal Firewall 2001 3.0.4.91	Norton Personal Firewall/ Internet Security 2001 Buffer Overflow CVE Name: CAN-2002-0663	High	CyberNotes-2002-15
Symantec ²⁰¹⁹	Windows 98/NT 4.0/2000, XP, Unix	Enterprise Firewall 6.5.2 NT/2000, 7.0 Solaris, 7.0 NT/2000, Gateway Security 5110, 5200, 5300, Ghost Corporate Edition 7.5, Raptor Firewall 6.5 Windows NT, 6.5.3 Solaris, Veloci Raptor 1.0, 1.1, 1.5	Multiple Symantec Product Weak TCP Initial Sequence Numbers Randomization	Medium	CyberNotes-2002-16
Symantec ²⁰²⁰	Windows 98/ME/NT 3.5/4.0/2000	Norton AntiVirus 2001	Norton Antivirus 2001 Poproxy Username Denial of Service	Low	CyberNotes-2002-19

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Symantec ²⁰²¹	Windows NT 4.0/2000, Unix	Enterprise Firewall 6.5.2 NT/2000, 7.0 Solaris, 7.0 NT/2000, Gateway Security 5110, 5200, 5300, Raptor Firewall 6.5 Windows NT, 6.5.3 Solaris, Veloci Raptor 1000, 1100, 1200, 1300, 500, 700	Multiple Symantec HTTP Proxy Remote Denial of Service	Low	CyberNotes-2002-21
Symantec ²⁰²²	Windows NT 4.0/2000, Unix	Enterprise Firewall 6.5.2 NT/2000, Raptor Firewall 6.5 Windows NT, Raptor Firewall 6.5.3 Solaris	Multiple Symantec HTTP Proxy Information Disclosure	Medium	CyberNotes-2002-21
Symantec ²⁰²³	Multiple	Norton AntiVirus Corporate Edition 7.5, 7.6, 7.51	Symantec NAVCE Privilege Escalation	High	CyberNotes-2002-21
Symantec ²⁰²⁴	Multiple	Veloci Raptor 1.0, 1.1, 1.5, 1200, 1300	VelociRaptor Denial of Service	Low/High (High if DDoS best practices not in place)	CyberNotes-2002-21
Symantec ²⁰²⁵	Multiple	Java! JustInTime Compiler 210.65	Symantec Java! JustInTime Compiler Command Execution	High	CyberNotes-2002-24
Symatec ²⁰²⁶	Multiple	popper_mod 1.0, 1.2, 1.2.1	Popper_Mod Default Administrative Access	Medium	CyberNotes-2002-07
Synthetic Reality ²⁰²⁷	Unix	Sympoll 1.2	Sympoll File Disclosure	Medium	CyberNotes-2002-16
T. Hauck ²⁰²⁸	Windows 95/98/ME/NT 4.0/2000	Jana WebServer 1.0, 1.45, 1.46, 2.0, 2.0 Beta 1&2, 2.2.1	Jana WebServer Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information is obtained)	CyberNotes-2002-16
TalentSoft ²⁰²⁹	Windows 95/98/NT 4.0, Unix	TalentSoft Web+ Server 4.6, 5.0	TalentSoft Web+ Buffer Overflow	High	CyberNotes-2002-05
TalentSoft ²⁰³⁰	Windows 95/98/NT 4.0/2000, Unix	Web+ Server 4.6, 5.0	Web+ Buffer Overflow	High	CyberNotes-2002-06
TalentSoft ²⁰³¹	Windows 95/98/NT 4.0/2000, Unix	Web+ Server 5.0	Web+ WML Buffer Overflow	High	CyberNotes-2002-08
Tarantella, Inc. ²⁰³²	Unix	Enterprise 3 3.01, 3.0, 3.10, 3.11, 3.20	Enterprise 3 Race Condition	Medium	CyberNotes-2002-03
Tarantella, Inc. ²⁰³³	Unix	Enterprise 3 3.0, 3.0, 3.10, 3.11, 3.20	Enterprise 3 Symbolic Link	High	CyberNotes-2002-04
Tarantella, Inc. ²⁰³⁴	Unix	Enterprise 3 3.10, 3.11, 3.20	Enterprise 3 Install.CGI Sensitive Information	Medium	CyberNotes-2002-08
Teekai ²⁰³⁵	Multiple	Forum 1.2	Forum Multiple Vulnerabilities	Medium/High (High if administrative access can be obtained)	CyberNotes-2002-12
Teekai ²⁰³⁶	Multiple	Tracking Online 1.0	Tracking Online Cross-Site Scripting	Medium	CyberNotes-2002-12
Tel Condex Software ²⁰³⁷	Windows NT	SimpleWebServer 2.06	SimpleWeb Server Remote Denial of Service	Low	CyberNotes-2002-21
Telindus ²⁰³⁸	Multiple	1110 ADSL Router, 1120 ADSL Router	1100 Series Router Administration Password Leak	Medium	CyberNotes-2002-12
TFTPD32 ²⁰³⁹	Windows 95/98/NT 4.0/2000, XP	TFTPD32 2.50, 2.50.2	TFTPD32 Arbitrary File Download/ Upload	High	CyberNotes-2002-24
TFTPD32 ²⁰⁴⁰	Windows 95/98/NT 4.0/2000, XP	TFTPD32 2.50, 2.50.2	TFTPD32 Buffer Overflow	High	CyberNotes-2002-24
Thatware ²⁰⁴¹	Multiple	Thatware 0.5.3	Thatware Cross-Site Scripting	Medium	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
The Magic Notebook ²⁰⁴²	Unix	The Magic Notebook 1.0 b, 1.1 b	The Magic Notebook Remote Denial of Service	Low	CyberNotes-2002-23
The XMB Group ²⁰⁴³	Multiple	XMB Forum 1.6x	XMB Cross-Site Scripting	High	CyberNotes-2002-05
The XMB Group ²⁰⁴⁴	Multiple	XMB Forum 1.6 Magic Lantern	XMB Forum Magic Lantern Log File	Medium	CyberNotes-2002-10
The XMB Group ²⁰⁴⁵	Multiple	XMB Forum 1.6 Magic Lantern	XMB Forum Magic Lantern Cross-Site Scripting	High	CyberNotes-2002-12
Thorsten Korner ²⁰⁴⁶	Unix	123tkShop 0.2, 0.3	123tkShop Arbitrary File Include	Medium	CyberNotes-2002-15
Thorsten Korner ²⁰⁴⁷	Unix	123tkShop 0.2, 0.3, 0.3.1	123tkShop SQL Injection	High	CyberNotes-2002-15
Thunderstone ²⁰⁴⁸	Multiple	Texis 3.0	Texis Path Disclosure	Medium	CyberNotes-2002-03
Tight Auction ²⁰⁴⁹	Multiple	TightAuction 3.0	TightAuction Configuration File Information Disclosure	Medium	CyberNotes-2002-20
TightVNC ²⁰⁵⁰	Multiple	TightVNC 1.2 .0, 1.2.1	TightVNC Repeated Challenge	Medium	CyberNotes-2002-15
Timecop ²⁰⁵¹	Unix	WMCube/GDK 0.98	WMCube/ GDK Object File Buffer Overflow	High	CyberNotes-2002-01
tinc ²⁰⁵²	Unix	tinc 1.0pre3, 1.0pre3	tinc Multiple Vulnerabilities	Medium	CyberNotes-2002-01
Tiny Software ²⁰⁵³	Windows 95/98/ME/NT 4.0/2000, XP	Personal Firewall 2.0.15	Tiny Personal Firewall Unauthorized Access	Medium	CyberNotes-2002-05
Tiny Software ²⁰⁵⁴	Windows NT	Personal Firewall 3.0, 3.0.5, 3.0.6	Tiny Personal Firewall Log File Viewing Denial Of Service	Low/High (High if DDoS best practices not in place)	CyberNotes-2002-17
TkMail ²⁰⁵⁵	Unix	TkMail 4.0 beta9, beta8, beta6, beta4, beta1	TkMail Insecure Temporary Files	Medium	CyberNotes-2002-21
Todd Miller ^{2056, 2057, 2058, 2059, 2060, 2061, 2062}	Unix	Sudo 1.6.3- 1.6.3p7	Sudo Environment Variable	High	CyberNotes-2002-02
Tolis Group ²⁰⁶³	Unix	BRU 17.0 Linux	BRU Insecure Temporary File	Medium	CyberNotes-2002-03
Tolis Group ²⁰⁶⁴	Unix	BRU 17.0 Linux	BRU Race Condition	High	CyberNotes-2002-19
Tomahawk Technologies ²⁰⁶⁵	Windows NT 4.0/2000	SteelArrow Web Application Server 4.1	SteelArrow Multiple Buffer Overflow Vulnerabilities	High	CyberNotes-2002-17
Total PC Solutions ²⁰⁶⁶	Multiple	PHP Rocket Add-in for FrontPage 1.0	PHP Rocket Add-in for FrontPage Directory Traversal	Medium	CyberNotes-2002-01
TransSoft ²⁰⁶⁷	Windows 95/98/NT 4.0/2000	Broker FTP Server 5.0	Broker FTP Denial of Service	Low	CyberNotes-2002-11
Transware ²⁰⁶⁸	Multiple	Active! Mail 1.422, Mail 2.0	Active Mail HTML Injection	High	CyberNotes-2002-12
Trend Micro, Inc. ²⁰⁶⁹	Windows NT 3.5/3.5.1/ 4.0, Unix	InterScan VirusWall (HP-UX) 3.6, (Linux) 3.6, (Solaris) 3.6, VirusWall for Windows NT 3.51	InterScan VirusWall Scan Circumvention	Medium	CyberNotes-2002-06
Trend Micro, Inc. ²⁰⁷⁰	Unix	InterScan eManager 3.6 For Sun & Linux	InterScan eManager Bcc Disclosure	Medium	CyberNotes-2002-09
Trend Micro, Inc. ²⁰⁷¹	Windows NT 4.0	InterScan VirusWall for Windows NT 3.52	InterScan VirusWall SMTP Header Removal	Medium	CyberNotes-2002-11
Trend Micro, Inc. ²⁰⁷²	Windows NT 4.0	InterScan VirusWall for Windows NT 3.52	InterScan VirusWall Space Gap Scan Bypass CVE Name: CAN-2002-0637	Medium	CyberNotes-2002-15
Trend Micro, Inc. ²⁰⁷³	Windows, Unix	InterScan VirusWall 3.52, InterScan VirusWall (Linux) 3.6	InterScan VirusWall HTTP 1.1 Transfer-Encoding & Content Encoding Bypass	Medium	CyberNotes-2002-19
Trend Micro, Inc. ²⁰⁷⁴	Multiple	InterScan VirusWall 3.6 Build 1182, 1.3.6	InterScan VirusWall Unauthorized Proxy Connections	Medium	CyberNotes-2002-25
Trend Micro, Inc. ²⁰⁷⁵	Windows 98/ME/2000XP	OfficeScan Corporate Edition 5.02, PC-cillin 2003, 2002, 2000	Trend Micro PC-cillin Mail Scanner Buffer Overflow	Low	CyberNotes-2002-25
Trevor Lee ²⁰⁷⁶	Multiple	SWServer 2.2	SWServer Directory Traversal	Medium	CyberNotes-2002-18
Trolltech Qt ²⁰⁷⁷	Multiple	Assistant 1.0	Trolltech Qt Assistant Default Port Unauthorized Access	Medium	CyberNotes-2002-20
Turnkey WebTools ²⁰⁷⁸	Multiple	SunShop Shopping Cart 1.5, 2.0-2.2, 2.4-2.5	SunShop Shopping Cart Cross-Site Scripting	High	CyberNotes-2002-08
TuxBR ²⁰⁷⁹	Unix	LIBCgi 1.0.2, 1.0.3	LIGCGI Buffer Overflow	High	CyberNotes-2002-24

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Ultimate PHP Board ²⁰⁸⁰	Multiple	Ultimate PHP Board 1.0 b, 1.0	Ultimate PHP Board Second 'admin' Account	Medium	CyberNotes-2002-18
Ultimate PHP Board ²⁰⁸¹	Multiple	Ultimate PHP Board 1.0, 1.0 b	Ultimate PHP Board Unauthorized Administrative Access	High	CyberNotes-2002-19
Ultimate PHP Board ²⁰⁸²	Unix	Ultimate PHP Board 1.0 b	Ultimate PHP Board Information Disclosure	Medium	CyberNotes-2002-20
Ultimate PHP Board ²⁰⁸³	Unix	Ultimate PHP Board 1.0 final beta	Ultimate PHP Board Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-25
Ultrafunk ²⁰⁸⁴	Windows 95/98/ME/NT 4.0/2000, XP	Popcorn 1.20	Popcorn Multiple Remote Denial of Service Vulnerabilities	Low	CyberNotes-2002-15
Understroem ²⁰⁸⁵	Unix	Instant Web Mail 0.59 & prior	Instant Web Mail POP3 Commands & Mail Filters	High	CyberNotes-2002-07
Uninet ²⁰⁸⁶	Windows, Unix	StatsPlus 1.25 Windows, 1.25 Unix	StatsPlus HTTP Header HTML Injection	High	CyberNotes-2002-15
Unisys ²⁰⁸⁷	Multiple	Clearpath	Unisys 'Clearpath' Denial of Service	Low	CyberNotes-2002-20
University of Cambridge ²⁰⁸⁸	Unix	Exim 3.34	Exim Buffer Overflow	Medium	CyberNotes-2002-04
University of Cambridge ²⁰⁸⁹	Unix	Exim 3.35, 3.36, 4.10	Exim Internet Mailer Format String	High	CyberNotes-2002-25
University of Cambridge ^{2090, 2091}	Unix	Exim 3.11-3.22, 3.30-3.33	Exim Pipe Hostname Arbitrary Command Execution	Medium	CyberNotes-2002-01
University of Kansas ²⁰⁹²	Multiple	Lynx 2.8.2 rel.1- 2.8.4 rel.1, 2.8.5 dev.8	Lynx Command Line URL CRLF Injection	Medium	CyberNotes-2002-17
University of Washington ²⁰⁹³	Unix	Pine 4.20, 4.21, 4.30, 4.33	Pine Environment Variable URL Shell Interpreting	High	CyberNotes-2002-01
University of Washington ²⁰⁹⁴	Unix	Pine 4.21, 4.30, 4.33, 4.44	Pine Unix Sensitive Information	Medium	CyberNotes-2002-12
University of Washington ²⁰⁹⁵	Unix	Pine 4.20, 4.21, 4.30, 4.33, 4.44	Pine Denial of Service	Low	CyberNotes-2002-15
University of Washington ²⁰⁹⁶	Unix	Pine 3.98, 4.0.2, 4.0.4, 4.10, 4.20, 4.21, 4.30, 4.33, 4.44	Pine From: Field	Low/High (High if arbitrary code can be executed)	CyberNotes-2002-23
USANet Creations ²⁰⁹⁷	Unix	MakeBid Auction Deluxe 3.30	MakeBid Auction Plaintext Login and Cross-Site Scripting	Medium High (High if arbitrary code can be executed)	CyberNotes-2002-04
Usermin/ Webmin ²⁰⁹⁸	Unix	Usermin 0.7, 0.80, 0.90; Webmin 0.91, 0.92-1, 0.92, 0.93, 9.4, 9.50, 9.60	Webmin/ Usermin Authentication Bypass	Medium	CyberNotes-2002-10
Usermin/ Webmin ²⁰⁹⁹	Unix	Usermin 0.7, 0.80, 0.90; Webmin 0.91, 0.92-1, 0.92, 0.93, 9.4, 9.50, 9.60	Webmin/ Usermin Login Cross-Site Scripting	High	CyberNotes-2002-10
UTStarcom ²¹⁰⁰	Multiple	BAS-1000 3.1 .10	BAS-1000 Default User Account Passwords	High	CyberNotes-2002-18
Valve Software ²¹⁰¹	Windows 95/98/ME/NT 4.0, Unix	Half-Life 1.1.0.9, 1.1.0.8, 1.1.0.4 Windows, 1.1.0.4 Linux, 1.1.1.0, Dedicated Server 3.1 & previous, 3.1.3 x	Half-Life Server New Player Flood Denial Of Service	Low	CyberNotes-2002-13
Van Dyke Technologies ²¹⁰²	Windows 98/98/ME/NT 4.0/2000, XP	SecureCRT 3.4-3.4.5, 4.0 beta	SecureCRT Buffer Overflow	High	CyberNotes-2002-15
VBulletin ²¹⁰³	Unix	VBulletin 2.0 rc 3, 2.0 rc 2, 2.2.0-2.2.4	VBulletin Cross-Site Scripting	High	CyberNotes-2002-06

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
VBulletin ²¹⁰⁴	Unix	VBulletin 2.2.0-2.2.2, 2.0 rc 2, 2.0 rc 3	VBulletin Cross-Site Scripting	High	CyberNotes-2002-06
VBulletin ²¹⁰⁵	Windows, Unix	VBulletin 2.2.7, 2.2.8	VBulletin HTML Injection	High	CyberNotes-2002-25
VBZoom ²¹⁰⁶	Windows, Unix	VBZoom 1.0 1	VBZoom Arbitrary File Upload	High	CyberNotes-2002-21
VBZoom ²¹⁰⁷	Windows, Unix	VBZoom 1.0 1	VBZoom Remote SQL Injection	High	CyberNotes-2002-21
Veridis ²¹⁰⁸	Multiple	OpenKey Server 1.2	OpenKey Server Cross-Site Scripting	High	CyberNotes-2002-07
Veritas Software ²¹⁰⁹	Windows NT 4.0/2000, Unix	Cluster Server 1.2 NT, 1.3 Solaris, 1.3 HP-UX, 1.3	Veritas Cluster Server Root Compromise	High	CyberNotes-2002-19
Verity ²¹¹⁰	Multiple	Search97 2.1	Verity Search97 Error Page Cross Site Scripting	High	CyberNotes-2002-13
ViewCVS ²¹¹¹	Unix	ViewCVS 0.8-0.9.2	ViewCVS Cross-Site Scripting	High	CyberNotes-2002-11
Vincent Courcelle ²¹¹²	Multiple	Trackeur de visiteurs 1.0	Trackeur De Visiteurs Tracking Evasion	Medium	CyberNotes-2002-09
Virtual Programming ²¹¹³	Windows 95/98/NT 4.0/2000, XP	VP-ASP 4.0	VP-ASP Multiple Vulnerabilities	Medium	CyberNotes-2002-11
Virtualzone ²¹¹⁴	Windows	SmartMail Server 1.0 BETA 10	SmartMail Denial of Service	Low	CyberNotes-2002-22
Virtualzone ²¹¹⁵	Windows	SmartMail Server 2.0	SmartMail Denial of Service	Low	CyberNotes-2002-22
Visual Shapers ²¹¹⁶	Multiple	ezContents 1.40, 1.41	ezContents Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-15
VMWare ²¹¹⁷	Windows NT	GSX Server 2.0	GSX Server Buffer Overflow	High	CyberNotes-2002-15
Voxel Dot Net ²¹¹⁸	Multiple	CBMS 0.7	CBMS Multiple Cross-Site Scripting	High	CyberNotes-2002-12
vpopmail-CGIApps ²¹¹⁹	Unix	vpopmail-CGIApps 0.2	vpopmail-CGIApps Insufficient Sanitization	High	CyberNotes-2002-22
vqSoft ²¹²⁰	Windows 95/98/NT 4.0	vqServer for Windows 1.9, 1.9.30, 1.9.47, 1.9.55	vqServer CGI Demo Program Script Injection	High	CyberNotes-2002-09
VTun ²¹²¹	Unix	VTun 2.0-2.4, 2.5b1	VTun ECB Mode Encryption	Medium	CyberNotes-2002-01
W3C ²¹²²	Windows 2000	Jigsaw 2.2.1	Jigsaw Device Name Path Disclosure	Medium	CyberNotes-2002-15
W3C ²¹²³	Windows 2000	Jigsaw 2.2.1	Jigsaw DOS Device Denial of Service	Low	CyberNotes-2002-15
W3C ²¹²⁴	Multiple	CERN httpd 3.0	W3C CERN httpd Proxy Cross-Site Scripting	High	CyberNotes-2002-17
W3C ²¹²⁵	Multiple	Jigsaw 2.2	Jigsaw Proxy Server Cross-Site Scripting	High	CyberNotes-2002-17
W3Perl ²¹²⁶	Windows NT 4.0/2000, Unix	W3Perl 2.81-2.85	W3Perl Log File	High	CyberNotes-2002-02
WASD ²¹²⁷	Multiple	WASD HTTP Server 7.1-7.2.3, 8.0	Multiple OpenVMS WASD HTTP Server Vulnerabilities	Medium/High (High if root is compromised)	CyberNotes-2002-20
Washing-ton University ²¹²⁸	Unix	wu-imapd 2000.0, 2000.0a-c, 2001.0, 2001.0a	Wu-imapd Remote Buffer Overflow	High	CyberNotes-2002-10
Washing-ton University ²¹²⁹	Multiple	wu-imapd 2001.0a	IMAP Arbitrary File Access	Medium	CyberNotes-2002-12
Watch Guard ²¹³⁰	Multiple	SOHO Firewall 5.0.35	SOHO Firewall IP Restrictions	Medium	CyberNotes-2002-08
Watch Guard ²¹³¹	Multiple	Rapid Stream 8000, 6000, 500, 4000, 2000; Watch Guard Firebox V10, V100, V60, V80	WatchGuard Firebox VClass CLI Interface Vulnerabilities	High	CyberNotes-2002-20

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Watch Guard ²¹³²	Multiple	SOHO Firewall prior to 5.0.35	SOHO Firewall Denial of Service	Low/High (High if DDoS best practices not in place)	CyberNotes-2002-08
Watch Guard ²¹³³	Multiple	Firebox Firmware 5.0	Firebox DVCP Remote Denial Of Service	Low	CyberNotes-2002-14
Watch Guard ²¹³⁴	Multiple	Soho Firewall, firmware 5.0.35a	Soho FTP Authentication	Medium/High (High if firewall control can be obtained)	CyberNotes-2002-14
Web Server Creator ²¹³⁵	Multiple	Web Server Creator Web Portal 0.1	Web Server Creator Web Portal Remote File Include	High	CyberNotes-2002-24
WebEasy Mail ²¹³⁶	Windows NT	WebEasy Mail 3.4.2.2	WebEasyMail Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information is obtained)	CyberNotes-2002-17
Webmin ²¹³⁷	Unix	Webmin 0.91	Webmin Directory Traversal	Medium	CyberNotes-2002-01
Webmin ²¹³⁸	Unix	Webmin 0.1-0.7, 0.8.3, 0.8.4, 0.21, 0.22, 0.31, 0.41, 0.42, 0.51, 0.76-0.80, 0.85, 0.88, 0.91, 0.92, 0.92-1	Webmin Script Code Input Validation	High	CyberNotes-2002-06
Webmin ²¹³⁹	Unix	Webmin 0.92, 0.92-1	Webmin Directory Permissions	High	CyberNotes-2002-06
Webmin ²¹⁴⁰	Unix	Webmin 0.93 & prior	Webmin Plaintext Authentication	Medium	CyberNotes-2002-07
Webmin ²¹⁴¹	Unix	Webmin 0.21, 0.22, 0.31, 0.41, 0.42, 0.51, 0.76-0.80, 0.85, 0.88, 0.91-0.990	Webmin CGI Improper Permissions	High	CyberNotes-2002-18
Webmin ²¹⁴²	Unix	Webmin 0.21, 0.22, 0.31, 0.41, 0.42, 0.51, 0.76-0.80, 0.85, 0.88, 0.91-0.990, 1.0.00	Webmin Static SSL Key	Medium	CyberNotes-2002-21
WebScripts ²¹⁴³	Multiple	WebBBS 4.0-4.2, 4.10-4.12, 4.20-4.22, 4.30-4.33, 5.0	WebBBS Remote Command Execution	High	CyberNotes-2002-13
Webscriptworld ²¹⁴⁴	Windows	Web Shop Manager 1.1	Web Shop Manager Search Box Improper Validation	High	CyberNotes-2002-17
WebSight Directory System ²¹⁴⁵	Unix	WebSight Directory System 0.1	WebSight Directory System Cross-Site Scripting	High	CyberNotes-2002-07
Webster ²¹⁴⁶	Windows 95/98/ME/ NT 4.0/2000, XP	Webster HTTP Server	Webster HTTP Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-25
WebTrends ²¹⁴⁷	Windows NT 4.0/2000	Reporting Center for Windows 4.0d	Reporting Center Buffer Overflow	High	CyberNotes-2002-08
William Deich ²¹⁴⁸	Unix	Super 3.12, 3.16-3.18	Super SysLog Format String	High	CyberNotes-2002-16
Windowmaker ²¹⁴⁹	Unix	Windowmaker 0.20.1-3, 0.52-2, 0.53, 0.61, 0.61.1, 0.62, 0.62.1, 0.63, 0.63.1, 0.64, 0.65, 0.80	WindowMaker Image Handling Buffer Overflow	High	CyberNotes-2002-23
wliang ²¹⁵⁰	Unix	wmtv 0.6.5	WMTV Buffer Overflow Vulnerabilities	High	CyberNotes-2002-03
WN Server ²¹⁵¹	Multiple	WN Server 1.18.2- 1.18.7, 1.19.0-1.19.9, 2.0.0	WN Server Buffer Overflow CVE Name: CAN-2002-1166	High	CyberNotes-2002-20
Wolfram Research ²¹⁵²	Windows, Unix	Web Mathematica Amateur 4.0, Professional 4.0	Web Mathematica Directory Traversal	Medium	CyberNotes-2002-13
WoltLab ²¹⁵³	Unix	Burning Board 1.1.1	Burning Board Randomization Function	Medium	CyberNotes-2002-11
WoltLab ²¹⁵⁴	Multiple	Burning Board 1.1.1	Burning Board URL Parameter Manipulation	Medium	CyberNotes-2002-08

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
WoltLab GbR ²¹⁵⁵	Unix	Burning Board 2.0 RC1, 2.0 beta 3-5	Burning Board Board.PHP SQL Injection	Medium/High (High if administrative access can be obtained)	CyberNotes-2002-19
Wordtrans ^{2156,2157}	Unix	Wordtrans-web 1.0 beta-2-2.4, 1.1 pre8	Wordtrans-web Remote Command Execution CVE Name: CAN-2002-0837	High	CyberNotes-2002-19
WorkforceROI ²¹⁵⁸	Multiple	Xpede 4.1, 7.0	Xpede Password Exposure	Medium	CyberNotes-2002-06
WorkforceROI ²¹⁵⁹	Windows	Xpede 4.1	Xpede Multiple Vulnerabilities	Medium	CyberNotes-2002-09
Working Resources Inc. ²¹⁶⁰	Windows 95/98/ME/NT 4.0/2000, XP	BadBlue 1.5	BadBlue Denial of Service	Low	CyberNotes-2002-02
Working Resources Inc. ²¹⁶¹	Windows 95/98/ME/NT 4.0/2000, XP	Deerfield D2Gfx 1.0.2; BadBlue 1.2.7, 1.2.8, 1.5, 1.5.6beta, 1.6.1beta, Enterprise Edition 1.5	BadBlue Cross-Site Scripting	High	CyberNotes-2002-05
Working Resources Inc. ²¹⁶²	Windows 95/98/ME/NT 4.0/2000, XP	Deerfield D2Gfx 1.0.2; BadBlue Enterprise Edition 1.5.6 Beta, 1.6 Beta, Personal Edition 1.5.6 Beta, 1.6 Beta	BadBlue Directory Traversal	Medium	CyberNotes-2002-05
Working Resources Inc. ²¹⁶³	Windows 95/98/ME/NT 4.0/2000, XP	BadBlue 1.7 .0	BadBlue Directory Contents Disclosure	Medium	CyberNotes-2002-12
Working Resources Inc. ²¹⁶⁴	Windows 95/98/ME/NT 4.0/2000, X P	BadBlue Enterprise Edition 1.7, Personal Edition 1.7	BadBlue EXT.DLL Cross-Site Scripting	High	CyberNotes-2002-13
Working Resources Inc. ²¹⁶⁵	Windows 95/98/ME/NT 4.0/2000, XP	BadBlue Personal Edition 1.7.3	BadBlue cleanSearch String() Cross-Site Scripting	High	CyberNotes-2002-14
Working Resources Inc. ²¹⁶⁶	Windows 95/98/ME/NT 4.0/2000, XP	BadBlue Personal Edition 1.7.3	BadBlue Denial of Service Vulnerabilities	Low	CyberNotes-2002-14
Working Resources Inc. ²¹⁶⁷	Windows 95/98/ME/NT 4.0/2000, XP	BadBlue Enterprise Edition 1.7, 1.7.2-1.7.4, BadBlue Personal Edition 1.7, 1.7.2-1.7.4	BadBlue 302 Message Cross-Site Scripting	High	CyberNotes-2002-15
Working Resources Inc. ²¹⁶⁸	Windows 95/98/ME/NT 4.0/2000, XP, Unix	BadBlue Enterprise Edition 1.7.3, BadBlue Personal Edition 1.7.3	BadBlue Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information is obtained)	CyberNotes-2002-15
Working Resources Inc. ²¹⁶⁹	Windows 95/98/ME/NT 4.0/2000, XP	BadBlue Enterprise Edition 1.7, 1.7.2-1.7.4	BadBlue Administrative Interface Arbitrary File Access	Medium	CyberNotes-2002-15.
Working Resources Inc. ²¹⁷⁰	Windows 98/2000	BadBlue 1.7 .0	BadBlue Access Control Circumvention	Medium	CyberNotes-2002-22
Working Resources Inc. ²¹⁷¹	Multiple	BadBlue 1.7.1	Working Resources BadBlue Search Page Cross Site Scripting	High	CyberNotes-2002-24
Working Resources Inc. ²¹⁷²	Windows NT	BadBlue 1.7.1	BadBlue Information Disclosure	Medium	CyberNotes-2002-24
WorldSpan ²¹⁷³	Windows 95/98	Res Manager 4.1	Res Manager Denial of Service	Low	CyberNotes-2002-14
WSMP3 ²¹⁷⁴	Multiple	WSMP3 .1, .2	WSMP3 Multiple Vulnerabilities	High	CyberNotes-2002-24
WWWIis ²¹⁷⁵	Unix	WWWIis 3.3, 3.45	WWWIis Remote Command Execution & File Disclosure	Medium/High (High if arbitrary code can be executed)	CyberNotes-2002-07
Xbreaky ²¹⁷⁶	Unix	Xbreaky .3, .4	Xbreaky Symbolic Link	Medium	CyberNotes-2002-19

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
X-Chat ²¹⁷⁷	Unix	X-Chat 1.4.2, 1.4.3	X-Chat CTCP Ping Arbitrary Remote IRC Command Execution	Medium	CyberNotes-2002-01
X-Chat ²¹⁷⁸	Unix	X-Chat 1.8.1, 1.8.6-1.8.8	XChat DNS Command Execution	High	CyberNotes-2002-07
X-Crew ²¹⁷⁹	Multiple	Ultimate PHP Board 1.0 Beta, 1.1	Ultimate PHP Board Multiple Vulnerabilities	Medium	CyberNotes-2002-09
X-Crew ²¹⁸⁰	Multiple	Ultimate PHP Board 1.0 Beta, 1.1	Ultimate PHP Board Image Tag Script Injection	High	CyberNotes-2002-09
x-dev ²¹⁸¹	Multiple	xNewsletter 1.0	xNewsletter Form Field Input Validation	High	CyberNotes-2002-08
Xerox Corporation ²¹⁸²	Multiple	DocuTech 6110, 6115	DocuTech Printer & Document Scanner Insecure Default Configuration	Medium	CyberNotes-2002-11
Xerox Corporation ²¹⁸³	Windows	DocuShare 2.2	Xerox DocuShare Vulnerabilities	Medium	CyberNotes-2002-20
Xerver ²¹⁸⁴	Windows 95/98/NT 4.0/2000, XP	Xerver 2.10	Xerver Denial of Service and Directory Traversal	Low/ Medium (Medium for the Directory Traversal vulnerability)	CyberNotes-2002-06
XFree86 ²¹⁸⁵	Unix	X11R6 4.0, 4.0.1, 4.0.2-11, 4.0.3, 4.1.0, 4.1-12, 4.1-11, 4.2.0	X Window System Denial of Service	Low	CyberNotes-2002-12
Ximian ²¹⁸⁶	Unix	Evolution 1.0.3-1.0.8	Evolution SSL Certificate	Medium	CyberNotes-2002-20
Ximian ^{2187, 2188}	Unix	Evolution 1.0.3, 1.0.4	Evolution Mailer Denial of Service	Low	CyberNotes-2002-10
Xinet ²¹⁸⁹	MacOS, Unix	K-AShare 11.01 IRIX	K-AShare Insecure Permissions	Medium	CyberNotes-2002-03
Xinetd ^{2190, 2191}	Unix	Xinetd 2.3.4-2.3.6	Xinetd Remote Denial of Service	Low	CyberNotes-2002-17
Xoops ²¹⁹²	Unix	Xoops 1.0 RC1	Xoops SQL 'userinfo.php' Sensitive Information	Medium	CyberNotes-2002-03
Xoops ²¹⁹³	Unix	Xoops 1.0 RC1	Xoops Private Message Box Cross-Site Scripting	High	CyberNotes-2002-03
Xoops ²¹⁹⁴	Unix	Xoops 1.0 RC3	XOOPS HTML Injection	High	CyberNotes-2002-20
Xoops ²¹⁹⁵	Unix	WebChat 0.6	Xoops WebChat Module Remote SQL Injection	High	CyberNotes-2002-23
Xoops ²¹⁹⁶	Windows, Unix	Xoops 1.3.5	Xoops Private Message System Font Attributes HTML Injection	High	CyberNotes-2002-25
Xqus ²¹⁹⁷	Multiple	X-News 1.0, 1.1	X-News Insecure User Database Permissions	High	CyberNotes-2002-06
Xqus ²¹⁹⁸	Multiple	X-Stat 2.2, 2.3	X-Stat Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-06
Xtell ²¹⁹⁹	Unix	Xtell 2.6.1	XTell Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	CyberNotes-2002-05
YaBB ²²⁰⁰	Windows 95/98/NT 4.0/2000	YaBB 1 Gold Release, 1 Gold - SP 1, 9.1.2000, 9.11.2000	YaBB Cross-Site Scripting	High	CyberNotes-2002-01
YaBB ²²⁰¹	Windows 95/98/NT 4.0/2000	YaBB 1 Gold Release	YaBB Flash File Script Injection	High	CyberNotes-2002-12
YaBB ²²⁰²	Unix	YaBB 1 Gold - SP 1	YaBB Gold Cross-Site Scripting	High	CyberNotes-2002-13
YaBB ²²⁰³	Windows, Unix	YaBB 1.40 1.41	YaBB Cross-Site Scripting	High	CyberNotes-2002-22
YaBB ²²⁰⁴	Unix	YaBB 1 Gold - SP 1	YaBB.pl Cross-Site Scripting	High	CyberNotes-2002-24
Yahoo! ²²⁰⁵	Windows 95/98/NT 4.0/2000, XP	Yahoo! Messenger 5.0	Yahoo! Messenger Multiple Vulnerabilities	Low	CyberNotes-2002-05

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
Yahoo! ²²⁰⁶	Windows 95/98/ME/NT 4.0/2000, XP	Instant Messenger 5.0	Instant Messenger Multiple Vulnerabilities	High	CyberNotes-2002-11
Yahoo! ²²⁰⁷	Multiple	Messenger 5.0 .1232, 5.0 .1046	Yahoo! Messenger Invisible User Circumvention	Medium	CyberNotes-2002-23
YAMAGUCHI ²²⁰⁸	Unix	Shingo beep2 1.0a, beep2 1.0, beep2 1.1, beep2 1.2	Shingo beep2 Command Line	Medium	CyberNotes-2002-02
Yann Ramin ²²⁰⁹	Unix	ATPhttpd 0.4 b	ATPhttpd Buffer Overflow Vulnerabilities	Medium	CyberNotes-2002-15
Yann Ramin ²²¹⁰	Unix	ATPhttpd 0.4, 0.4 b	ATP httpd Buffer Overflow	High	CyberNotes-2002-21
YoungZ Soft ²²¹¹	Multiple	Cmail Server 3.30	CMailServer Buffer Overflow	High	CyberNotes-2002-11
Zack Coburn ²²¹²	Unix	Meunity Community System 1.0	Meunity IMG Tag	High	CyberNotes-2002-21
Zap Book ²²¹³	Unix	Zap Book 1.0.3	Zap Book Server Side Include Arbitrary Command Execution & Script Injection	High	CyberNotes-2002-14
ZenTrack ²²¹⁴	Multiple	ZenTrack 2.0.1 c Beta, 2.0.2c Beta, 2.0.3	ZenTrack Information Disclosure	Medium	CyberNotes-2002-12
Zero One Tech ²²¹⁵	Multiple	P100s PrintServer 5.31.13E	ZOT P100s PrintServer SNMP Community String	Medium	CyberNotes-2002-05
Zeroboard ²²¹⁶	Unix	Zeroboard 4.1 pl2	Zeroboard PHP Include File Arbitrary Command Execution	High	CyberNotes-2002-13
ZeusTechnologies ²²¹⁷ <i>Upgrade now available</i> ²²¹⁸	Multiple	Zeus Web Server 4.1r2	Zeus Web Server Cross-Site Scripting	High	CyberNotes-2002-23 CyberNotes-2002-24
ZMailer ²²¹⁹	Unix	ZMailer 2.99.45- 2.99.51	ZMailer IPv6 Resolved Hostname Buffer Overflow	High	CyberNotes-2002-18
Zoltan Milosevic ²²²⁰	Multiple	Fluid Dynamics Search Engine 2.0.0.0050-2.0.0.0054	Fluid Dynamics Search Engine Cross-Site Scripting	High	CyberNotes-2002-14
Zone Labs ²²²¹	Windows 98/ME/NT 4.0/2000, XP	ZoneAlarm 3.0	ZoneAlarm MailSafe Filtering Bypass	Medium	CyberNotes-2002-07
Zope ²²²²	Unix	Zope 2.2.0-2.2.5, 2.3.0-2.3.3, 2.4.0-2.4.4b1, 2.5.0, 2.5.1b1	Zope Proxy Elevated Privileges	Medium	CyberNotes-2002-05
Zope ²²²³	Unix	Zope 2.1.x, 2.1.1, 2.1.7, 2.2.0, 2.2 beta1, 2.2-2.2.5, 2.3.0-2.3.3, 2.4.0-2.4.4 b1, 2.5.0, 2.5.1 b1, 2.5.1	Zope "Through The Web" Remote Denial of Service CVE Name: CAN-2002-0687	Low	CyberNotes-2002-20
Zope ²²²⁴	Windows, Unix	Zope 2.3.2, 2.3.3, 2.4.0-2.4.3, 2.4.4 b1, 2.5.0, 2.5.1	Zope XML-RPC Request	Medium	CyberNotes-2002-20
Zope ²²²⁵	Unix	Zope 2.1.1, 2.1.7, 2.2.0, 2.2-2.2.5, 2.3.0-2.3.3, 2.4.0-2.5.1, 2.6.0b1	Zope Failed Login	Medium	CyberNotes-2002-21
Zope ^{2226, 2227}	Unix	Zope 2.4.0-2.4.3, 2.4.4 b1, 2.5.0, 2.5.1	Zope ZCatalog Plug-In Access Control CVE Name: CAN-2002-0688	Medium	CyberNotes-2002-20
ZyXel ²²²⁸	Multiple	Prestige 681	ZyXel Prestige SDSL Router IP Fragment Reassembly	Low	CyberNotes-2002-01
ZyXel ²²²⁹	Multiple	Zywall10 0.0V3.50 (WA.1), 0.0V3.24 (WA.2), (WA.1), (WA.0), 0.0V3.20 (WA.1), (WA.0)	Zywall10 Denial of Service	Low	CyberNotes-2002-06
ZyXel ²²³⁰	Multiple	Prestige 642R	Prestige 642R Malformed Packet Denial of Service	Low	CyberNotes-2002-13
ZyXel ²²³¹	Multiple	Prestige 310, 642R	Prestige Router Malformed TCP Packet Denial of Service	Low	CyberNotes-2002-15

*"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 – medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a “High” threat.

Viruses

The following table provides the reader with a year-end summary of the top ten high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available.** The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), and approximate date first found. During the year, a number of anti-virus vendors have included information on Trojan Horses and Worms. *NOTE: At times, Trojans may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Date
1	W32/Klez	Worm	January 2002
2	W32/SirCam	Worm	July 2001
3	W32/Nimda-A-O	File, Worm	September 2001
4	W32/BadTrans	Worm	April 2001
5	Elkern	File Infector	October 2001
6	W32/Magistr	File, Worm	March 2001
7	W32/Hybris	File, Worm	November 2000
8	W32/Yaha	Worm	February 2002
9**	Funlove	File	November 1999
9	W32/Bugbear-A	Worm	September 2002
10	JS/NoClose	Trojan	May 2002

** Note: Two viruses tied for the ninth ranking position.

Trojans

“Trojan Horse programs”, or Trojans, have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans in 2002 gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a summary list of Trojans that have received write-ups in during the past year in CyberNotes. A version number is provided where relevant. *NOTE: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
AdClicker-J	N/A	CyberNotes-2002-25
AIM-Flood	N/A	CyberNotes-2002-16
APSTrojan.sl	N/A	CyberNotes-2002-03
Arial	N/A	CyberNotes-2002-08
Backdoor.AIMVision	N/A	CyberNotes-2002-21
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.AntiLam.20	20	CyberNotes-2002-18
Backdoor.Antilam.g1	g1	CyberNotes-2002-23
Backdoor.Armageddon.B	N/A	CyberNotes-2002-20
Backdoor.Asniffer	N/A	CyberNotes-2002-21
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Assasin.B	B	CyberNotes-2002-23
Backdoor.Assasin.C	C	CyberNotes-2002-24
Backdoor.Baste	N/A	CyberNotes-2002-23
Backdoor.Bofishy.C	C	CyberNotes-2002-23
Backdoor.Cabro	N/A	CyberNotes-2002-17
Backdoor.Cabrotor	N/A	CyberNotes-2002-18
Backdoor.Cigivip	N/A	CyberNotes-2002-23
Backdoor.Coreflood	N/A	CyberNotes-2002-25
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Cyn	N/A	CyberNotes-2002-18
Backdoor.DarkFtp	N/A	CyberNotes-2002-19
Backdoor.DarkSky.B	B	CyberNotes-2002-20
Backdoor.DarkSky.C	C	CyberNotes-2002-21
Backdoor.Delf	N/A	CyberNotes-2002-16
Backdoor.Delf.B	B	CyberNotes-2002-16
Backdoor.Delf.C	C	CyberNotes-2002-17
Backdoor.Delf.D	D	CyberNotes-2002-22
Backdoor.Delf.E	E	CyberNotes-2002-24
Backdoor.Denwp	N/A	CyberNotes-2002-25
Backdoor.Dindang	N/A	CyberNotes-2002-22
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	N/A	CyberNotes-2002-16
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Elitem	N/A	CyberNotes-2002-20

Trojan	Version	CyberNotes Issue #
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Expjan	N/A	CyberNotes-2002-18
Backdoor.Feardoor	N/A	CyberNotes-2002-21
Backdoor.Fearic	N/A	CyberNotes-2002-16
Backdoor.FTP_Ana	N/A	CyberNotes-2002-20
Backdoor.FTP_Ana.B	B	CyberNotes-2002-20
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.Fulamer.25	25	CyberNotes-2002-24
Backdoor.FunFactory	N/A	CyberNotes-2002-19
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.GF.13	13	CyberNotes-2002-23
Backdoor.Gchoice.12	12	CyberNotes-2002-25
Backdoor.Goster	N/A	CyberNotes-2002-20
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.GWGhost	N/A	CyberNotes-2002-21
Backdoor.Hatckel	N/A	CyberNotes-2002-25
Backdoor.Helios	N/A	CyberNotes-2002-19
Backdoor.Hupigeon	N/A	CyberNotes-2002-21
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.IrcContact	N/A	CyberNotes-2002-24
Backdoor.Kaitex.B	B	CyberNotes-2002-20
Backdoor.Kaitex.C	C	CyberNotes-2002-22
Backdoor.Kavar	N/A	CyberNotes-2002-16
Backdoor.Klb	N/A	CyberNotes-2002-22
Backdoor.Kryost	N/A	CyberNotes-2002-18
Backdoor.Lanfilt	N/A	CyberNotes-2002-24
Backdoor.Lanfiltrator	N/A	CyberNotes-2002-25
Backdoor.Laphex	N/A	CyberNotes-2002-18
Backdoor.Laphex.Client	N/A	CyberNotes-2002-18
Backdoor.Lastdoor	N/A	CyberNotes-2002-18
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Latinus.B	B	CyberNotes-2002-18
Backdoor.Litmus.203.b	203.b	CyberNotes-2002-22
Backdoor.Litmus.2a	2a	CyberNotes-2002-20
Backdoor.LittleWitch.B	B	CyberNotes-2002-22
Backdoor.Lolok	N/A	CyberNotes-2002-25
Backdoor.Malpayo	N/A	CyberNotes-2002-24
Backdoor.Mapsy	N/A	CyberNotes-2002-25
Backdoor.Miffice	N/A	CyberNotes-2002-18
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.Miranda	N/A	CyberNotes-2002-25
Backdoor.Mite	N/A	CyberNotes-2002-18
Backdoor.MLink	N/A	CyberNotes-2002-16
Backdoor.Ndad	N/A	CyberNotes-2002-17
Backdoor.Neodurk	N/A	CyberNotes-2002-23
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Niovadoor	N/A	CyberNotes-2002-22
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	B	CyberNotes-2002-11
Backdoor.Optix.04	04	CyberNotes-2002-19
Backdoor.Optix.04.b	04.b	CyberNotes-2002-22

Trojan	Version	CyberNotes Issue #
Backdoor.Optix.04.c	C	CyberNotes-2002-22
Backdoor.OptixPro.10	10	CyberNotes-2002-18
Backdoor.OptixPro.11	11	CyberNotes-2002-20
Backdoor.OptixPro.11.b	11.b	CyberNotes-2002-22
Backdoor.OptixPro.12	12	CyberNotes-2002-18
Backdoor.Osirdoor	N/A	CyberNotes-2002-17
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.Pest.Cli	N/A	CyberNotes-2002-20
Backdoor.Pestdoor	N/A	CyberNotes-2002-20
Backdoor.Phoenix	N/A	CyberNotes-2002-19
Backdoor.Platrash	N/A	CyberNotes-2002-21
Backdoor.Ptakks.B	B	CyberNotes-2002-18
Backdoor.RCServ	N/A	CyberNotes-2002-19
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.RemoteNC.B	B	CyberNotes-2002-24
Backdoor.Revrs	N/A	CyberNotes-2002-22
Backdoor.Ripjac	N/A	CyberNotes-2002-24
Backdoor.RMFDoor.Cli	N/A	CyberNotes-2002-20
Backdoor.Robi	N/A	CyberNotes-2002-18
Backdoor.Roxrat.10	10	CyberNotes-2002-20
Backdoor.Roxrat.12	12	CyberNotes-2002-25
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Scanboot	N/A	CyberNotes-2002-17
Backdoor.Sdbot.B	B	CyberNotes-2002-22
Backdoor.Seamy	N/A	CyberNotes-2002-18
Backdoor.Singu	N/A	CyberNotes-2002-22
Backdoor.Skun	N/A	CyberNotes-2002-25
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Sparta.B	B	CyberNotes-2002-19
Backdoor.Sparta.C	C	CyberNotes-2002-21
Backdoor.Spigot.B	B	CyberNotes-2002-22
Backdoor.Spoofbot	N/A	CyberNotes-2002-24
Backdoor.StealthEye	N/A	CyberNotes-2002-25
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Synrg	N/A	CyberNotes-2002-22
Backdoor.Systsec	N/A	CyberNotes-2002-04
Backdoor.Tela	N/A	CyberNotes-2002-17
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Theef.B	B	CyberNotes-2002-21
Backdoor.Theef.C	C	CyberNotes-2002-25
Backdoor.Tourniq	N/A	CyberNotes-2002-25
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.VB.CH	N/A	CyberNotes-2002-25
Backdoor.WinShell	N/A	CyberNotes-2002-16
Backdoor.Wiween	N/A	CyberNotes-2002-22
Backdoor.Wold	N/A	CyberNotes-2002-22
Backdoor.Y3KRat.14	14	CyberNotes-2002-24
Backdoor.Y3KRat.15	15	CyberNotes-2002-17
Backdoor.Zenmaster	N/A	CyberNotes-2002-19
BackDoor-AAB	AAB	CyberNotes-2002-02
BackDoor-ABH	ABH	CyberNotes-2002-06

Trojan	Version	CyberNotes Issue #
BackDoor-ABN	ABN	CyberNotes-2002-06
Backdoor-AKO	AKO	CyberNotes-2002-20
BackDoor-AKR	AKR	CyberNotes-2002-19
BackDoor-AKW	AKW	CyberNotes-2002-25
BackDoor-ALT	ALT	CyberNotes-2002-21
BackDoor-AMB	AMB	CyberNotes-2002-22
BackDoor-AMH	AMH	CyberNotes-2002-23
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	201	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/EHKSLogger	N/A	CyberNotes-2002-19
BDS/Osiris	N/A	CyberNotes-2002-06
BDS/Pestdoor.4	4	CyberNotes-2002-20
BDS/SDbot.XY	XV	CyberNotes-2002-25
BDS/Sporkbot	N/A	CyberNotes-2002-20
BDS/WinSpyer	N/A	CyberNotes-2002-22
BKDR_EMULBOX.A	A	CyberNotes-2002-10
BKDR_INTRUZZO.A	A	CyberNotes-2002-09
BKDR_LITMUS.C	C	CyberNotes-2002-09
BKDR_SMALLFEG.A	A	CyberNotes-2002-04
BKDR_WARHOME.A	A	CyberNotes-2002-06
Bneo.Trojan	N/A	CyberNotes-2002-18
Cardst	N/A	CyberNotes-2002-17
Cytron	N/A	CyberNotes-2002-20
Dewin	N/A	CyberNotes-2002-08
Diskfill-F	F	CyberNotes-2002-23
DIder	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader.BO.dr	BO.dr	CyberNotes-2002-24
Downloader-BO.b	BO.b	CyberNotes-2002-23
Downloader-W	W	CyberNotes-2002-08
FakeGina.Trojan	N/A	CyberNotes-2002-16
Fortnight	N/A	CyberNotes-2002-10
Hacktool.IPStealer	N/A	CyberNotes-2002-02
IIS.Beavuh-Exploit	N/A	CyberNotes-2002-17
IRC.kierz	N/A	CyberNotes-2002-16
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
Jekord	N/A	CyberNotes-2002-19
JS/NoClose	N/A	CyberNotes-2002-11
JS/Seeker-E	E	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
Liquid.Trojan	N/A	CyberNotes-2002-14
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	CX	CyberNotes-2002-08
Netbus.160.Dropper	N/A	CyberNotes-2002-17
Poldo	N/A	CyberNotes-2002-25
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-MSNcrack	N/A	CyberNotes-2002-18
PWS-MSNSteal	N/A	CyberNotes-2002-17
PWS-Ritter	N/A	CyberNotes-2002-16
PWSteal.Antigen	N/A	CyberNotes-2002-23

Trojan	Version	CyberNotes Issue #
PWSteal.Avisa	N/A	CyberNotes-2002-24
PWSteal.BStroj	N/A	CyberNotes-2002-20
PWSteal.Fender	N/A	CyberNotes-2002-25
PWSteal.Kaylo	N/A	CyberNotes-2002-17
PWSteal.Netsnake	N/A	CyberNotes-2002-17
PWSteal.Profman	N/A	CyberNotes-2002-17
PWSteal.SoopSpy	N/A	CyberNotes-2002-18
QDel227	227	CyberNotes-2002-09
QDel234	234	CyberNotes-2002-11
QDel297	297	CyberNotes-2002-23
QDel350	350	CyberNotes-2002-24
QDel356	356	CyberNotes-2002-25
RCServ	N/A	CyberNotes-2002-10
Reboot-R	R	CyberNotes-2002-18
Reboot-T	T	CyberNotes-2002-25
SecHole.Trojan	N/A	CyberNotes-2002-01
StartPage-B	B	CyberNotes-2002-16
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/EvilDX	N/A	CyberNotes-2002-19
Tr/FakeYahoMe	N/A	CyberNotes-2002-23
Tr/Mastaz	N/A	CyberNotes-2002-23
Tr/SCKeYLog.Spy.20	20	CyberNotes-2002-22
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/WLoader	N/A	CyberNotes-2002-20
TR/Zirko	N/A	CyberNotes-2002-10
Trj/GhostGirl	N/A	CyberNotes-2002-19
Troj/Apher-A	A	CyberNotes-2002-17
Troj/Bdoor-AML	AML	CyberNotes-2002-23
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/Download-A	A	CyberNotes-2002-01
Troj/DSS-A	A	CyberNotes-2002-12
Troj/FireAnv-A	A	CyberNotes-2002-19
Troj/Flood-O	O	CyberNotes-2002-14
Troj/ICQBomb-A	A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	B	CyberNotes-2002-11
Troj/Msstake-A	A	CyberNotes-2002-03
Troj/Netdex-A	A	CyberNotes-2002-21
Troj/Nethief-C	C	CyberNotes-2002-22
Troj/Optix-03-C	03-C	CyberNotes-2002-01
Troj/Ritter-A	A	CyberNotes-2002-17
Troj/Sub7-21-I	21-I	CyberNotes-2002-01
Troj/Tobizan-A	A	CyberNotes-2002-16
Troj/Tubmo-A	A	CyberNotes-2002-25
Troj/Unreal-A	A	CyberNotes-2002-16
Troj/WebDL-E	E	CyberNotes-2002-01
Troj/Zasil-A	A	CyberNotes-2002-23
TROJ_CYN12.B	B	CyberNotes-2002-02
TROJ_DANSCHL.A	A	CyberNotes-2002-01
TROJ_DOAL.A	A	CyberNotes-2002-14
TROJ_DSNX.A	A	CyberNotes-2002-03
TROJ_FLOOD.BI.DR	N/A	CyberNotes-2002-25

Trojan	Version	CyberNotes Issue #
TROJ_FRAG.CLI.A	A	CyberNotes-2002-02
TROJ_ICONLIB.A	A	CyberNotes-2002-03
TROJ_INOR.A	A	CyberNotes-2002-23
TROJ_INOR.B	B	CyberNotes-2002-23
TROJ_JUNTADOR.B	B	CyberNotes-2002-06
TROJ_JUNTADOR.G	G	CyberNotes-2002-10
TROJ_OPENME.B	B	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
TROJ_SMBNUKE.A	A	CyberNotes-2002-18
TROJ_SQLSPIDA.B	B	CyberNotes-2002-11
TROJ_SUOMIA.A	A	CyberNotes-2002-18
TROJ_WORTRON.10B	10B	CyberNotes-2002-12
Trojan.Adclicker	N/A	CyberNotes-2002-19
Trojan.Adnap	N/A	CyberNotes-2002-17
Trojan.Ahero	N/A	CyberNotes-2002-24
Trojan.Allclicks.A	A	CyberNotes-2002-13
Trojan.AntiUpdater	N/A	CyberNotes-2002-23
Trojan.Avid	N/A	CyberNotes-2002-19
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Crabox	N/A	CyberNotes-2002-17
Trojan.DiabKey	N/A	CyberNotes-2002-18
Trojan.Diskfil	N/A	CyberNotes-2002-19
Trojan.Downloader.Cile	N/A	CyberNotes-2002-25
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Houpe	N/A	CyberNotes-2002-23
Trojan.Iblis	N/A	CyberNotes-2002-22
Trojan.IrcBounce	N/A	CyberNotes-2002-19
Trojan.Junnan	N/A	CyberNotes-2002-16
Trojan.Lovead	N/A	CyberNotes-2002-19
Trojan.Nullbot	N/A	CyberNotes-2002-19
Trojan.Portacopo.br	N/A	CyberNotes-2002-16
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.Ajim_bbs	N/A	CyberNotes-2002-19
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.PWS.QQPass.C	C	CyberNotes-2002-21
Trojan.Starfi	N/A	CyberNotes-2002-16
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
Trojan.Win32.Filecoder	N/A	CyberNotes-2002-18
Trojan.Win32.MSNTrick	N/A	CyberNotes-2002-17
Trojan.WinReboot	N/A	CyberNotes-2002-20
UNIX_ALUTAPS.A	A	CyberNotes-2002-21
VBS.AVFake	N/A	CyberNotes-2002-22
VBS.Gascript	N/A	CyberNotes-2002-04
VBS.Krim.C	C	CyberNotes-2002-22
VBS.Lavra.B.Worm	N/A	CyberNotes-2002-19
VBS.Zevach	N/A	CyberNotes-2002-15
VBS/Helvis	N/A	CyberNotes-2002-22
VBS_CHICK.B	B	CyberNotes-2002-07
VBS_THEGAME.A	A	CyberNotes-2002-03

Trojan	Version	CyberNotes Issue #
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Azak	N/A	CyberNotes-2002-16
W32.Balick.Trojan	N/A	CyberNotes-2002-24
W32.Cbomb	N/A	CyberNotes-2002-16
W32.Click	N/A	CyberNotes-2002-15
W32.Darkgoose.Trojan	N/A	CyberNotes-2002-24
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	N/A	CyberNotes-2002-16
W32.Kotef	N/A	CyberNotes-2002-16
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Manifest.Trojan	N/A	CyberNotes-2002-24
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.STD.D	N/A	CyberNotes-2002-22
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15
Worm/Garra	N/A	CyberNotes-2002-20
X97M.Feng.A.Trojan	N/A	CyberNotes-2002-25

-
- 1 SecurityFocus, April 29, 2002.
 - 2 Securiteam, September 30, 2001.
 - 3 Bugtraq, April 30, 2002.
 - 4 Bugtraq, May 27, 2002.
 - 5 Bugtraq, December 2, 2002.
 - 6 Securiteam, December 5, 2002.
 - 7 iXsecurity Security Vulnerability Report, 20020404, May 3, 2002.
 - 8 Bugtraq, June 18, 2002.
 - 9 Blackshell Security Advisory No2, December 31, 2001.
 - 10 iDEFENSE Security Advisory, 11.01.02, October 31, 2002.
 - 11 ACD Incorporated Security Advisory, January 22, 2002.
 - 12 Bugtraq, May 10, 2002.
 - 13 Securiteam, November 24, 2002.
 - 14 Securiteam, November 24, 2002.
 - 15 SecurityFocus, April 25, 2002.
 - 16 INetCop Security Advisory, 2002-0x82-001, November 11, 2002.
 - 17 Securiteam, January 5, 2002.
 - 18 Bugtraq, January 15, 2002.
 - 19 Sec-Tec Advisory 24.10.02, October 24, 2002.
 - 20 Illegal Instruction Labs Advisory, September 25, 2002.
 - 21 RUS-CERT Advisory, 2002-02:01, February 12, 2002.
 - 22 Bugtraq, December 25, 2001.
 - 23 Securiteam, February 16, 2002.
 - 24 SecurityFocus, April 29, 2002.
 - 25 Vulnerability Note, VU#116875, February 19, 2002.
 - 26 Securiteam, June 21, 2002.
 - 27 Securiteam, July 31, 2002.
 - 28 Bugtraq, July 19, 2002.
 - 29 Securiteam, March 8, 2002.
 - 30 Bugtraq, September 3, 2002.
 - 31 Netric Security Team Advisory, September 4, 2002.
 - 32 Bugtraq, January 7, 2002.
 - 33 Securiteam, December 22, 2001.

34 Securiteam, January 29, 2002.
35 Bugtraq, December 5, 2002.
36 Bugtraq, December 18, 2001.
37 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:083-22, June 3, 2002.
38 Hewlett-Packard Company Security Bulletin, HPSBTL0602-047, June 5, 2002.
39 Caldera International, Inc. Security Advisory, CSSA-2002-026.0, June 11, 2002.
40 SecurityFocus, August 30, 2002.
41 SecurityTracker Alert ID, 1005727, November 29, 2002.
42 Securiteam, January 17, 2002.
43 SecurityBugware Advisory, February 19, 2002.
44 CERT Advisory CA-2002-32, November 21, 2002.
45 Bugtraq, November 12, 2002.
46 Securiteam, March 26, 2002.
47 Bugtraq, January 8, 2002.
48 KPMG-2002013, April 18, 2002.
49 Macromedia Security Bulletin, MPSB02-03, June 13, 2002.
50 Bugtraq, November 20, 2002.
51 Securiteam, September 24, 2002.
52 Bugtraq, October 27, 2002.
53 Bugtraq, May 27, 2002.
54 Bugtraq, January 20, 2002.
55 Bugtraq, December 31, 2001.
56 w00w00 Security Development, January 2, 2002.
57 NTBugtraq, January 6, 2002.
58 NTBugtraq, February 24, 2002.
59 NtWaK0 & Recon Advisory, February 29, 2002.
60 INTEXXIA(c) Security Advisory, 1052-300102, April 16, 2002.
61 Bugtraq, April 16, 2002.
62 Bugtraq, April 21, 2002.
63 Bugtraq, May 8, 2002.
64 Bugtraq, May 6, 2002.
65 Bugtraq, July 16, 2002.
66 SecurityFocus, August 18, 2002.
67 Bugtraq, October 21, 2002.
68 Bugtraq, November 25, 2002.
69 Bugtraq, November 17, 2002.
70 Bugtraq, June 20, 2002.
71 Debian Security Advisory, DSA 125-1, March 28, 2002.
72 Bugtraq, June 13, 2002.
73 Foundstone Labs, FS-062502-22-AXSH, June 25, 2002.
74 Foundstone Security Advisory, FS-070102-23-AXPR, July 1, 2002.
75 Qitest1 Security Advisory #005, July 18, 2002.
76 Debian Security Advisory, DSA 177-1, October 17, 2002.
77 Securiteam, October 21, 2002.
78 SNS Advisory No.57, October 28, 2002.
79 SecurityFocus, April 25, 2002.
80 Bugtraq, April 6, 2002.
81 Bugtraq, January 6, 2002.
82 Securiteam, January 4, 2002.
83 Bugtraq, February 7, 2002.
84 Bugtraq, March 21, 2002.
85 CHINANSL Security Team, April 22, 2002.
86 Securiteam, April 20, 2002.
87 Procheckup Security Bulletin, PR02-05, May 29, 2002.
88 Procheckup Security Bulletin, PR02-07, May 29, 2002.
89 Procheckup Security Bulletin, PR02-06, May 29, 2002.
90 Vulnwatch, June 11, 2002.
91 KPMG-2002024, June 19, 2002.
92 KPMG-2002025, June 20, 2002.
93 Westpoint Security Advisory, wp-02-0008, July 10, 2002.
94 Apache Software Foundation, August 9, 2002.
95 SecurityFocus, August 16, 2002.
96 SecurityFocus, August 21, 2002.
97 SecurityTracker, September 26, 2002.
98 Bugtraq, September 23, 2002.
99 Bugtraq, October 16, 2002.
100 Debian Security Advisory, DSA 187-1, November 4, 2002.
101 Debian Security Advisory, DSA 188-1, November 5, 2002.
102 Debian Security Advisory, DSA 195-1, November 13, 2002.

103 Georgi Guninski Security Advisory #58, November 6, 2002.
104 Qualys Security Advisory, QSA-2002-12-04, December 4, 2002.
105 Bugtraq, September 24, 2002.
106 Gentoo Linux Security Announcement, September 25, 2002.
107 Bugtraq, December 6, 2002.
108 ECHU Alert #2, September 25, 2002.
109 Bugtraq, October 2, 2002.
110 Bugtraq, September 23, 2002.
111 SecurityFocus, December 29, 2001.
112 Securiteam, January 16, 2002.
113 SecurityFocus, February 21, 2002.
114 Shadow Penguin Security (SPS) Advisory #46, February 9, 2002.
115 SecurityTracker Alert ID 1004317, May 17, 2002.
116 SecurityFocus, June 28, 2002.
117 Bugtraq, July 13, 2002.
118 Bugtraq, July 24, 2002.
119 Bugtraq, September 13, 2002.
120 @stake Inc. Security Advisory, a091002-1, September 10, 2002.
121 Apple Security Update, 120150, September 24, 2002.
122 UkR Security Team, October 26, 2002.
123 SecurityFocus, December 7, 2002.
124 Bugtraq, April 10, 2002.
125 Bugtraq, July 29, 2002.
126 INetCop Security Advisory, 2002-0x82-009, December 10, 2002.
127 Bugtraq, February 8, 2002.
128 Bugtraq, February 9, 2002.
129 Bugtraq, October 29, 2002.
130 Team N.finity Security Advisory, July 3, 2002.
131 Bugtraq, August 4, 2002.
132 Bugtraq, October 7, 2002.
133 ALPER Research Labs Security Advisory, ARL02-A07, March 16, 2002.
134 Bugtraq, November 8, 2002.
135 Bugtraq, January 15, 2002.
136 SecurityFocus, May 4, 2002
137 SecurityFocus, May 4, 2002.
138 Securiteam, May 4, 2002
139 SecurityFocus, April 10, 2002.
140 SecurityFocus, April 10, 2002.
141 Bugtraq, February 12, 2002.
142 SecurityTracker Alert ID 1005523, November 3, 2002.
143 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:026-43, March 21, 2002.
144 Netric Security Team, September 19, 2002.
145 ITCF Advisory 13, April 29, 2002.
146 VIGILANTe Advisory 2001003, December 21, 2001.
147 Bugtraq, July 17, 2002.
148 SecurityTracker Alert ID 1005401, October 10, 2002.
149 Avaya Security Advisory, July 22, 2002.
150 SecurityFocus, September 13, 2002.
151 Securiteam, October 17, 2002.
152 Bugtraq, March 18, 2002.
153 Bugtraq, February 21, 2002.
154 Strumpf Noir Society Advisories, January 17, 2002.
155 Gobbles Security Lab, June 12, 2002.
156 Vuln-Dev, January 21, 2002.
157 Debian Security Advisory, DSA 175-1, October 15, 2002.
158 EnGarde Secure Linux Security Advisory, ESA-20021016-025, October 16, 2002.
159 EnGarde Secure Linux Security Advisory, ESA-20021029-028, October 29, 2002.
160 SuSE Security Announcement, SuSE-SA:2002:039, October 31, 2002.
161 Capzlock Security Advisory No. 1, May 20, 2002.
162 Bugtraq, June 18, 2002.
163 Securiteam, February 17, 2002.
164 PenTest Limited Security Advisory, ptl-2002-03, July 1, 2002.
165 KPMG-2002003, January 8, 2002.
166 BEA Security Advisory, BEA02-03.03, April 30, 2002.
167 KPMG-2002016, April 30, 2002.
168 BEA Systems Inc. Security Advisory, BEA02-17.00, May 9, 2002.
169 BEA Systems Security Advisory, BEA02-18.00, May 13, 2002.
170 BEA Systems, Inc. Security Advisory, BEA00-06.00, June 24, 2002.
171 KPMG-2002029, July 8, 2002.

172 BEA Security Advisory, BEA02-20.00, September 26, 2002.
173 BEA Security Advisory, BEA02-21.00, October 1, 2002.
174 BEA Systems Security Advisory, BEA02-22.00, October 15, 2002.
175 Bugtraq, June 9, 2002.
176 Securiteam, August 27, 2002.
177 AresU Advisory, July 19, 2002.
178 AresU Advisory, July 18, 2002.
179 Bugtraq, October 27, 2002.
180 ALPER Research Labs Security Advisory, ARL02-A08, March 16, 2002.
181 Debian Security Advisory, DSA-138-1, August 1, 2002.
182 ALPER Research Labs Security Advisory, ARL02-A11, March 17, 2002.
183 SecurityFocus, April 30, 2002.
184 KPMG-2002005, March 18, 2002.
185 Bugtraq, June 9, 2002.
186 Bugtraq, June 9, 2002.
187 SecurityTracker Alert ID, 1005681, November 22, 2002.
188 Strumpf Noir Society Advisories, January 15, 2002.
189 ALPER Research Labs Security Advisory, ARL02-A06, March 12, 2002.
190 Bugtraq, July 1, 2002.
191 PPP-Design Advisory, April 28, 2002.
192 Blue Coat Systems Security Advisory, September 3, 2002.
193 Securiteam, February 18, 2002.
194 Strumpf Noir Society Advisories, February 13, 2002.
195 SecurityOffice, May 27, 2002.
196 Bugtraq, August 8, 2002.
197 Securiteam, January 8, 2002.
198 SecurityFocus, November 29, 2002.
199 Bugtraq, June 18, 2002.
200 Securiteam, September 26, 2002.
201 Bugtraq, February 27, 2002.
202 Securiteam, April 16, 2002.
203 SecurityFocus, May 4, 2002.
204 Phoenelit Advisory, July 27, 2002.
205 SecurityFocus, January 4, 2002.
206 Bugtraq, October 24, 2002.
207 Bugtraq, January 3, 2002.
208 Arhont Ltd. Information Security Advisory, November 13, 2002
209 FreeBSD Security Advisory, FreeBSD-SA-02:25, May 20, 2002.
210 SCO Security Advisory, CSSA-2002-039.0, October 29, 2002.
211 Svindel.net Security Advisory, January 8, 2002.
212 Bugtraq, February 19, 2002.
213 Bugtraq, July 24, 2002.
214 Bugtraq, May 6, 2002.
215 Bugtraq, August 13, 2002.
216 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.22, May 28, 2002.
217 Bugtraq, January 8, 2002.
218 Bugtraq, January 20, 2002.
219 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.3, February 7, 2002.
220 Bugtraq, February 10, 2002.
221 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.8, March 11, 2002.
222 Caldera International, Inc. Security Advisory, CSSA-2002-013.0, March 26, 2002.
223 Caldera International, Inc. Security Advisory, CSSA-2002-005.0, April 1, 2002.
224 Caldera International, Inc. Security Advisory, CSSA-2002-009.0, March 15, 2002.
225 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.15, April 11, 2002.
226 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.20, May 22, 2002.
227 Strategic Reconnaissance Team Security Advisory, SRT2002-06-04-1611, June 4, 2002.
228 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.23, May 30, 2002.
229 Caldera International, Inc. Security Advisory, CSSA-2002-024.0, June 3, 2002.
230 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.27, June 18, 2002.
231 SCO Security Advisory, CSSA-2002-SCO.38, August 27, 2002.
232 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.5.1, February 16, 2002.
233 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.18, May 8, 2002.
234 SCO Security Advisory, CSSA-2002-SCO.41, October 21, 2002.
235 Security Freaks Advisory, SFAD02-002, November 25, 2002.
236 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:246-18, December 4, 2002.
237 Securiteam, July 12, 2002.
238 Bugtraq, September 30, 2002.
239 CERT/CC Vulnerability Note, VU#740169, December 3, 2002.
240 Nth Dimension Security Advisory, NDSA20020719, July 19, 2002.

241 SecurityFocus, November 13, 2002.
242 Bugtraq, February 5, 2002.
243 Bugtraq, June 24, 2002.
244 KPMG-2002021, June 17, 2002.
245 KPMG-2002022, June 17, 2002.
246 KPMG-2002033, July 17, 2002.
247 Securiteam, March 16, 2002.
248 Securiteam, January 17, 2002.
249 Securiteam, February 25, 2002.
250 Securiteam, August 5, 2002.
251 Bugtraq, August 31, 2002.
252 Bugtraq, September 9, 2002.
253 NTBugtraq, September 19, 2002.
254 Bugtraq, September 18, 2002.
255 NTBugtraq, September 20, 2002.
256 ComputerSecurityNow Advisory, September 23, 2002.
257 Bugtraq, September 21, 2002.
258 NTBugtraq, September 22, 2002.
259 Bugtraq, May 17, 2002.
260 Bugtraq, March 25, 2002.
261 Bugtraq, April 8, 2002.
262 Bugtraq, April 23, 2002.
263 Bugtraq, June 11, 2002.
264 Bugtraq, May 29, 2002.
265 Bugtraq, March 8, 2002.
266 CheckPoint Security Alert, October 7, 2002.
267 Securiteam, September 3, 2002.
268 SecurityFocus, September 18, 2002.
269 GOBBLES Security Advisory, December 29, 2001.
270 SecurityFocus, January 16, 2002.
271 Mandrake Linux Security Update Advisory, MDKSA-2002:021, March 7, 2002.
272 FreeBSD Security Advisory, FreeBSD-SA-02:17, March 12, 2002.
273 Securiteam, January 23, 2002.
274 eSecurityOnline Security Advisory 2408, April 29, 2002.
275 Cisco Security Advisory, January 9, 2002.
276 HHC Network, January 3, 2002.
277 Cisco Security Advisory, January 16, 2002.
278 Bugtraq, January 30, 2002.
279 Cisco Security Advisory, February 12, 2002.
280 Cisco Security Advisory, 20020227, February 27, 2002.
281 Cisco Security Advisory, 20020327-1.2, March 29, 2002.
282 Cisco Security Advisory, 2002-04-03, April 3, 2002.
283 Cisco Security Advisory, 200204009, April 9, 2002.
284 SecurityFocus, April 17, 2002.
285 Bugtraq, May 9, 2002.
286 Cisco Security Advisory, May 15, 2002.
287 Cisco Security Advisory, May 17, 2002.
288 Cisco Security Advisory, May 16, 2002.
289 Cisco Security Advisory, May 15, 2002.
290 Bugtraq, May 20, 2002.
291 Cisco Security Advisory, May 23, 2002.
292 Securiteam, May 21, 2002.
293 Cisco Security Advisory, May 22, 2002.
294 Security Advisory, June 27, 2002.
295 Cisco Security Advisory, June 17, 2002.
296 Cisco Security Advisory, June 19, 2002.
297 sMax. Security Advisory, June 14, 2002.
298 Cisco Security Advisory, June 19, 2002.
299 Cisco Security Advisory, August 7, 2002.
300 Cisco Security Advisory, July 30, 2002.
301 Cisco Security Advisory, August 12, 2002.
302 Cisco Security Advisory, September 3, 2002.
303 Cisco Security Advisory, September 5, 2002.
304 Cisco Security Advisory, September 5, 2002.
305 Cisco Security Advisory, September 5, 2002.
306 Cisco Security Advisory, September 5, 2002.
307 Cisco Security Advisory, September 5, 2002.
308 SecurityFocus, September 19, 2002.
309 Cisco Security Advisory, September 18, 2002.

310 Cisco Security Advisory, September 18, 2002.
311 Cisco Security Advisory, 20021016, October 16, 2002.
312 Cisco Security Advisory Revision 1.1, October 5, 2002.
313 Cisco Security Advisory, 20021031, October 31, 2002.
314 Bugtraq, November 5, 2002.
315 Cisco Security Advisory, 20021120, November 20, 2002.
316 Cisco Security Advisory, 20021120, November 20, 2002.
317 Cisco Security Advisory, December 11, 2002.
318 Cisco Security Advisory, CI-02.02, February 7, 2002.
319 Bugtraq, March 9, 2002.
320 Kikkert Security Advisory, December 13, 2001.
321 Bugtraq, January 22, 2002.
322 Bugtraq, February 20, 2002.
323 Bugtraq, March 27, 2002.
324 Securiteam, March 28, 2002.
325 SecurityFocus, August 11, 2002.
326 Bugtraq, October 2, 2002.
327 Bugtraq, October 2, 2002.
328 Bugtraq, January 14, 2002.
329 Securiteam, March 9, 2002.
330 Bugtraq, October 14, 2002.
331 SecurityFocus, May 12, 2002.
332 Blackshell Advisory # 5, May 6, 2002.
333 SCAN Associates Sdn Bhd Security Advisory, July 23, 2002.
334 Securiteam, June 22, 2002.
335 Bugtraq, October 3, 2002.
336 Compaq Security Advisory, SSRT0799, February 18, 2002.
337 Compaq Security Advisory, SSRT0799, February 18, 2002.
338 Compaq Security Advisory, SSRT0813, February 25, 2002.
339 Compaq Security Advisory, SSRT-541, April 18, 2002.
340 Compaq Security Bulletin, SSRT2179, May 21, 2002.
341 Compaq Security Bulletin, SSRT0794U, July 16, 2002.
342 Compaq Security Bulletin, SSRT0795U, July 16, 2002.
343 Bugtraq, July 19, 2002.
344 Compaq Security Bulletin, SSRT2257, August 5, 2002.
345 Compaq Security Bulletin, SSRT2257, August 5, 2002.
346 Compaq Compute Corporation Advisory, SSRT2275/SSRT2229:, August 30, 2002.
347 Hewlett Packard Security Advisory, September 10, 2002.
348 Hewlett Packard Security Advisory, SSRT-547, September 11, 2002.
349 Hewlett Packard Security Advisory, SSRT2371, September 25, 2002.
350 Hewlett Packard Security Bulletin, SSRT2362, September 21, 2002.
351 SecurityFocus, September 23, 2002.
352 Hewlett Packard Security Advisory, SSRT2266, November 13, 2002.
353 Bugtraq, January 28, 2002.
354 Bugtraq, January 30, 2002.
355 SecurityFocus, January 31, 2002.
356 Bugtraq, August 30, 2002.
357 Bugtraq, April 5, 2002.
358 SecurityFocus, December 4, 2002.
359 Bugtraq, December 2, 2002.
360 Conectiva Linux Security Announcement, CLA-2002:455, January 18, 2002.
361 Securiteam, October 17, 2002.
362 Strumpf Noir Society Advisories, February 11, 2002.
363 Bugtraq, October 5, 2002.
364 Bugtraq, August 7, 2002.
365 Bugtraq, October 2, 2002.
366 Bugtraq, October 2, 2002.
367 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:081-06, May 10, 2002.
368 Nomad Mobile Research Centre Advisory, May 10, 2002.
369 Bugtraq, November 14, 2002.
370 DER ADV #8, May 25, 2002.
371 SecurityFocus, November 9, 2002.
372 Securiteam, January 22, 2002.
373 Bugtraq, December 9, 2002.
374 Securiteam, December 5, 2002.
375 Bugtraq, December 2, 2002.
376 Bugtraq, April 2, 2002.
377 Securiteam, January 22, 2002.
378 ECHU Alert #2, September 25, 2002.

379 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:186-07, August 28, 2002.
380 Debian Security Advisory, DSA 160-1, September 3, 2002.
381 Gentoo Linux Security Announcement, September 4, 2002.
382 Bugtraq, March 31, 2002.
383 SecurityFocus, October 19, 2002.
384 NetBSD Security Advisory, 2002-024, November 4, 2002.
385 Securiteam, May 28, 2002.
386 iDEFENSE Security Advisory, 06.10.2002, June 10, 2002.
387 Securiteam, December 19, 2001.
388 Bugtraq, March 9, 2002.
389 SecurityFocus, July 24, 2002.
390 Securiteam, January 3, 2002.
391 Guardeonic Solutions AG Security Advisory #01-2002, September 17, 2002.
392 Guardeonic Solutions AG Security Advisory #02-2002, September 17, 2002.
393 DCScripts Security Advisory, January 31, 2002.
394 ALPER Research Labs Security Advisory, ARL02-A02, February 15, 2002.
395 ALPER Research Labs Security Advisory, ARL02-A03, February 15, 2002.
396 Debian Security Advisory, DSA 117-1, March 5, 2002.
397 Debian Security Advisory, DSA-129-1, May 27, 2002.
398 Debian Security Advisory, DSA 202-2, December 6, 2002.
399 Debian Security Advisory, DSA 150-1, August 13, 2002.
400 Bugtraq, June 25, 2002.
401 Securiteam, April 4, 2002.
402 Securiteam, June 20, 2002.
403 Bugtraq, May 7, 2002.
404 Bugtraq, May 7, 2002.
405 Securiteam, December 12, 2002.
406 Securiteam, May 21, 2002.
407 SNS Advisory No.47, December 28, 2001.
408 Global InterSec LLC Advisory, 2002012101, February 7, 2002.
409 Bugtraq, June 14, 2002.
410 Demarc Security Update Advisory, April 16, 2002.
411 PivX Security Advisory, August 24, 2002.
412 iDEFENSE Security Advisory 09.18.2002, September 18, 2002.
413 iDEFENSE Security Advisory 09.18.2002, September 18, 2002.
414 SecurityFocus, April 25, 2002.
415 Bugtraq, December 21, 2001.
416 Phenoelit Advisory, July 27, 2002
417 Bugtraq, October 23, 2002.
418 ETHEREANET-NCC Security Report EN-NCC-20021014-04, October 21, 2002.
419 SecurityFocus, November 7, 2002.
420 Bugtraq, January 20, 2002.
421 PPP-Design Advisory, April 28, 2002.
422 SCAN Associates Sdn Bhd Security Advisory, July 29, 2002.
423 Securiteam, June 3, 2002.
424 Debian Security Advisory, DSA 197-1, November 15, 2002.
425 Gentoo Linux Security Announcement, 200211-005, November 19, 2002.
426 Securiteam, June 24, 2002.
427 ECHU Alert #2, September 25, 2002.
428 Bugtraq, May 31, 2002.
429 VulnWatch, October 21, 2002.
430 ITCP Advisory 7, April 3, 2002.
431 Securiteam, March 15, 2002.
432 SecurityFocus, May 28, 2002.
433 Securiteam, June 11, 2002.
434 Bugtraq, January 16, 2002.
435 DownBlood Security Research Lab Advisory, June 6, 2002.
436 SuSE Security Announcement, SuSE-SA:2002:043, November 12, 2002.
437 SuSE Security Announcement, SuSE-SA:2002:043, November 12, 2002.
438 Bugtraq, August 24, 2002.
439 Bugtraq, October 10, 2002.
440 Phoenix Sistemi Security Advisory, December 26, 2001.
441 Securiteam, April 6, 2002.
442 Bugtraq, April 10, 2002.
443 AIS advisory # 0005, September 29, 2002.
444 AIS advisory # 0004 September 29, 2002.
445 Bugtraq, July 29, 2002.
446 Securiteam, March 8, 2002.
447 Securiteam, January 17, 2002.

448 SecurityFocus, August 7, 2002.
449 ISS Security Alert Summary AS02-37, September 16, 2002.
450 NTBugtraq, July 10, 2002.
451 Bugtraq, July 3, 2002.
452 SecurityFocus, September 23, 2002.
453 bogofilter-SA-2002:01, November 29, 2002.
454 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:047-10, May 20, 2002.
455 Mandrake Linux Security Update Advisory, MDKSA-2002:036, May 28, 2002.
456 e-matters GmbH Security Advisory, 03/2002, September 29, 2002.
457 Gentoo Linux Security Announcement, October 1, 2002.
458 EnGarde Secure Linux Security Advisory, ESA-20021003-023, October 3, 2002.
459 Securiteam, June 5, 2002.
460 VulnWatch, January 10, 2002.
461 Bugtraq, February 5, 2002.
462 Bugtraq, February 26, 2002.
463 Security Advisory, enpa-sa-00004, May 19, 2002.
464 Conectiva Linux Security Announcement, CLA-2002:474, April 25, 2002.
465 Etheral Advisory, enpa-sa-00005, June 28, 2002.
466 Conectiva Linux Security Announcement, CLA-2002:505, July 4, 2002.
467 Etheral Security Advisory, enpa-sa-00006, August 20, 2002.
468 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:169-13, August 28, 2002.
469 FreeBSD Security Notice, FreeBSD-SN-02:05, August 28, 2002.
470 Gentoo Linux Security Announcement, August 30, 2002.
471 Securiteam, March 26, 2002.
472 Next Generation Security Technologies Security Advisory, NGSEC-2002-1, February 5, 2002.
473 Bugtraq, January 29, 2002.
474 Telhack 026 Inc. Security Advisory #3, May 30, 2002.
475 Bugtraq, November 10, 2002.
476 Securiteam, February 12, 2002.
477 SecurityFocus, July 15, 2002.
478 Bugtraq, August 31, 2002.
479 Bugtraq, July 29, 2002.
480 Securiteam, January 9, 2002.
481 Bugtraq, January 7, 2002.
482 Superpetz Advisory #002, February 4, 2002.
483 SecurityFocus, July 17, 2002.
484 Bugtraq, May 28, 2002.
485 Bugtraq, September 4, 2002.
486 Bugtraq, October 22, 2002.
487 Securiteam, April 4, 2002.
488 SecurityTracker Alert ID, 1005766, December 5, 2002.
489 Securiteam, March 22, 2002.
490 Securiteam, March 16, 2002.
491 KPMG-2002014, April 19, 2002.
492 Bugtraq, January 17, 2002.
493 Bugtraq, January 18, 2002.
494 Bugtraq, March 20, 2002.
495 Bugtraq, March 17, 2002.
496 Bugtraq, September 24, 2002.
497 ECHU Alert #2, September 25, 2002.
498 Bugtraq, September 25, 2002.
499 Bugtraq, October 10, 2002.
500 iDEFENSE Security Advisory, 10.31.02c, October 31, 2002.
501 Bugtraq, November 24, 2002.
502 Bugtraq, August 15, 2002.
503 iDEFENSE Security Advisory 11.06.02, November 6, 2002.
504 Debian Security Advisory, DSA 189-1, November 6, 2002.
505 Securiteam, July 31, 2002.
506 Securiteam October 1, 2002.
507 FreeBSD Security Advisory, FreeBSD-SA-02:01, January 7, 2002.
508 FreeBSD Security Advisory, FreeBSD-SA-02:07, January 18, 2002.
509 FreeBSD Security Advisory, FreeBSD-SA-02:09, February 6, 2002.
510 FreeBSD Security Advisory, FreeBSD-SA-02:20, April 16, 2002.
511 FreeBSD Security Advisory, FreeBSD-SA-02:21, April 17, 2002.
512 Bugtraq, May 18, 2002.
513 FreeBSD Security Advisory, FreeBSD-SA-02:24, May 20, 2002.
514 FreeBSD Security Advisory, FreeBSD-SA-02:26, May 29, 2002.
515 FreeBSD Security Advisory, FreeBSD-SA-02:27, May 29, 2002.
516 FreeBSD Security Advisory, FreeBSD-SA-02:35, August 5, 2002.

517 FreeBSD Security Advisory, FreeBSD-SA-02:36, August 6, 2002.
518 FreeBSD Security Advisory, FreeBSD-SA-02:37, August 6, 2002.
519 FreeBSD Security Advisory, FreeBSD-SA-02:38, August 18, 2002.
520 FreeBSD Security Notice, FreeBSD-SN-02:05, August 28, 2002.
521 iDEFENSE Security Advisory, September 16, 2002.
522 FreeBSD Security Advisory, FreeBSD-SA-02:39, September 16, 2002.
523 SecurityFocus, November 26, 2002.
524 Shadow Penguin Security #44, January 11, 2002.
525 Securiteam, January 14, 2002.
526 Bugtraq, February 18, 2002.
527 iDEFENSE Security Advisory, 09.23.2002, September 23, 2002.
528 Securiteam, September 12, 2002.
529 Procheckup Security Bulletin, PR02-12, May 29, 2002.
530 Bugtraq, February 27, 2002.
531 Bugtraq, June 21, 2002.
532 Bugtraq, August 14, 2002.
533 Vulnwatch, February 20, 2002.
534 Securiteam, October 15, 2002.
535 Netric Security Team, August 27, 2002.
536 Bugtraq, January 3, 2002.
537 Securiteam, January 17, 2002.
538 ALPER Research Labs Security Advisory, ARL02-A13, June 10, 2002.
539 Bugtraq, July 19, 2002.
540 iDEFENSE Security Advisory, 09.26.2002, September 26, 2002.
541 Gentoo Linux Security Announcement, 200210-003, October 17, 2002.
542 Debian Security Advisory, DSA 176-1, October 16, 2002.
543 Debian Security Advisory, DSA 179-1, October 18, 2002.
544 Debian Security Advisory, DSA 182-1, October 28, 2002.
545 Mandrake Linux Security Update Advisory, MDKSA-2002:069, October 22, 2002.
546 Mandrake Linux Security Update Advisory, MDKSA-2002:071, October 24, 2002.
547 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:212-06, October 4, 2002.
548 KDE Security Advisory, October 9, 2002.
549 Conectiva Linux Security Announcement, CLA-2002:542, November 6, 2002.
550 SCO Security Advisory, CSSA-2002-053.0, November 22, 2002.
551 Gentoo Linux Security Announcement, October 3, 2002.
552 "After" Security Advisory, ASA-0000, October 1, 3002.
553 KHAM SIN Security News, November 3, 2002.
554 Bugtraq, January 22, 2002.
555 Red Hat Security Advisory, RHSA-2002:004-06, January 14, 2002.
556 Securiteam, March 15, 2002.
557 Caldera International, Inc. Security Advisory, CSSA-2002-018.1, May 13, 2002.
558 Mandrake Linux Security Update Advisory, MDKSA-2002:031, May 16, 2002.
559 Gobblers Security Alert, April 21, 2002.
560 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:065-13, May 14, 2002.
561 Gentoo Linux Security Announcement, 200210-012, October 30, 2002.
562 Conectiva Linux Security Announcement, CLA-2002:489, May 24, 2002.
563 Conectiva Linux Security Announcement, CLA-2002:489, May 24, 2002.
564 Bugtraq, July 24, 2002.
565 Red Hat Security Advisory, RHSA-2002:012-06, January 17, 2002.
566 Debian Security Advisory, DSA-105-1, January 22, 2002.
567 Gentoo Linux Security Announcement, October 1, 2002.
568 Hewlett-Packard Company Security Bulletin, HPSBTL0209-068, October 1, 2002.
569 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:096-24, September 30, 2002.
570 Debian Security Advisory, DSA-209-1, December 13, 2002.
571 Mandrake Security Advisory, MDKSA-2002:086, December 11, 2002.
572 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:229-10, December 10, 2002.
573 Bugtraq, April 16, 2002.
574 Debian Security Advisory, DSA 114-1, February 21, 2002.
575 SuSE Security Announcement, SuSE-SA:2002:047, December 6, 2002.
576 Westpoint Security Advisory, wp-02-0001, July 10, 2002.
577 Securiteam, August 14, 2002.
578 GreyMagic Security Advisory, GM#001-MC, August 8, 2002.
579 Bugtraq, August 15, 2002.
580 SecurityTracker Alert ID, 1005650, November 18, 2002.
581 SecurityFocus, December 11, 2002.
582 Bugtraq, June 20, 2002.
583 Debian Security Advisory, DSA-095-1, December 27, 2001.
584 Securiteam, May 18, 2002.
585 Bugtraq, March 20, 2002.

586 RedHat Security Advisory, RHSA-2002:070-06, May 2, 2002.
587 Conectiva Linux Security Announcement, CLA-2002:477, May 3, 2002.
588 Bugtraq, May 17, 2002.
589 SecurityFocus, October 30, 2002.
590 Debian Security Advisory, DSA-205-1, December 10, 2002.
591 SCAN Associates Advisory, October 18, 2002.
592 Bugtraq, February 7, 2002.
593 SecurityFocus, May 29, 2002.
594 AngryPacket Security Advisory, January 3, 2002.
595 Securiteam List Digest, January 8, 2002.
596 Hewlett-Packard Company Security Bulletin, HPSBUX0201-178, January 7, 2002.
597 Hewlett-Packard Company Security Bulletin, HPSBUX0201-179, January 16, 2002.
598 Bugtraq, February 19, 2002.
599 Hewlett-Packard Company Security Bulletin, HPSBUX0203-186, March 8, 2002.
600 Bugtraq, February 28, 2002.
601 Hewlett-Packard Company Security Bulletin, HPSBMP0204-013, April 18, 2002.
602 Hewlett Packard Company Security Bulletin, HPSBMP0204-014, May 1, 2002.
603 Hewlett-Packard Company Security Bulletin, HPSBUX0205-193, May 7, 2002.
604 Securiteam, June 24, 2002.
605 Hewlett-Packard Company Security Bulletin, HPSBUX0208-206, August 6, 2002.
606 Phnoelit Advisory, July 27, 2002.
607 Hewlett-Packard Company Security Bulletin, HPSBUX0208-208, August 8, 2002.
608 Hewlett-Packard Company Security Bulletin, HPSBTL0208-059, August 13, 2002.
609 Hewlett-Packard Company Security Bulletin, HPSBTL0208-058, August 13, 2002.
610 Hewlett-Packard Company Security Bulletin, HPSBUX0208-0210, August 14, 2002.
611 Hewlett-Packard Company Security Bulletin, HPSBUX0208-0211, August 14, 2002.
612 Hewlett-Packard Company Security Bulletin, HPSBUX0208-213, August 27, 2002.
613 Hewlett-Packard Company Security Bulletin, HPSBUX0208-214, August 28, 2002.
614 iDEFENSE Security Advisory 09.18.2002, September 18, 2002.
615 Hewlett-Packard Company Security Bulletin, HPSBUX0209-221, September 30, 2002.
616 Hewlett Packard Security Bulletin, HPSBUX0209-220, September 23, 2002.
617 Hewlett Packard Systems Security Bulletin, SSRT2208, October 7, 2002.
618 Hewlett Packard Systems Security Advisory, HPSBUX0210-223, October 16, 2002.
619 Hewlett Packard Security Bulletin, SSRT2265, November 4, 2002.
620 Hewlett-Packard Company Security Bulletin, HPSBUX0212-232, December 10, 2002.
621 Hewlett-Packard Company Security Bulletin, HPSBUX0212-231, December 11, 2002.
622 Hewlett-Packard Company Security Advisory, HPSBUX0202-185, February 12, 2002.
623 Hewlett-Packard Company Security Advisory, HPSBUX0202-183, February 12, 2002.
624 Hewlett-Packard Company Security Bulletin, HPSBUX0203-189, March 22, 2002.
625 Bugtraq, April 15, 2002.
626 Hewlett-Packard Company Security Bulletin, HPSBUX0204-191, April 23, 2002.
627 Hewlett-Packard Company Security Bulletin, HPSBUX0205-192, May 7, 2002.
628 Hewlett-Packard Company Security Bulletin, HPSBUX0207-198, July 10, 2002.
629 Hewlett-Packard Company Security Bulletin, HPSBUX0207-196, July 2, 2002.
630 Hewlett-Packard Company Security Advisory, HPSBUX0207-0201, July 22, 2002.
631 Hewlett-Packard Company Security Advisory, HPSBUX0207-204, July 31, 2002.
632 Securiteam, July 28, 2002.
633 Securiteam, July 28, 2002.
634 Hewlett Packard Security Advisory, HPSBUX0209-219, September 25, 2002.
635 Hewlett Packard Security Advisory, SSRT2385, November 13, 2002.
636 Hewlett-Packard Company Security Bulletin, HPSBUX0212-227, December 3, 2002.
637 Hewlett-Packard Company Security Bulletin, HPSBUX0205-194, May 30, 2002.
638 Heysoft Security Bulletin, November 1, 2002.
639 HyperNikkiSystem Project, hns-SA-2002-01, February 14, 2002.
640 SecurityFocus, April 7, 2002.
641 Securiteam, January 8, 2002.
642 ALPER Research Labs Security Advisory, ARL02-A01, January 26, 2002.
643 Bugtraq, March 18, 2002.
644 Bugtraq, May 19, 2002.
645 Bugtraq, May 19, 2002.
646 Bugtraq, May 17, 2002.
647 Bugtraq, July 13, 2002.
648 Bugtraq, November 10, 2002.
649 Securiteam, March 4, 2002.
650 SecurityFocus, June 24, 2002.
651 INetCop Security Advisory, 2002-0x82-003, November 13, 2002.
652 Hughes Technology, November 25, 2002.
653 SecurityFocus, December 27, 2001.
654 Bugtraq, June 23, 2002.

655 HylaFAX.org Security Advisory, July 29, 2002.
656 KPMG-2002006, April 2, 2002.
657 Bugtraq, April 11, 2002.
658 Bugtraq, April 11, 2002.
659 iXsecurity Security Vulnerability Report, 20020328, April 11, 2002.
660 iXsecurity Security Vulnerability Report, 20020327, April 11, 2002.
661 IBM Security Advisory, MSS-OAR-E01-2002:318.1, May 24, 2002.
662 Bugtraq, May 30, 2002.
663 ptl-2002-05, July 15, 2002.
664 ptl-2002-04, July 15, 2002.
665 KPMG-2002035, September 19, 2002.
666 SecurityTracker, Alert ID 1005327, October 1, 2002.
667 Bugtraq, October 9, 2002.
668 Securiteam, October 1, 2002.
669 Securiteam, October 25, 2002.
670 Bugtraq, October 31, 2002.
671 Rapid 7, Inc. Security Advisory, R7-0007, October 23, 2002.
672 Rapid 7, Inc. Security Advisory, R7-0008, October 23, 2002.
673 SecurityTracker Alert ID, 1005604, November 12, 2002.
674 Bugtraq, November 13, 2002.
675 Bugtraq, April 4, 2002.
676 SecurityFocus, July 9, 2002.
677 Telhack 026 Inc. Security Advisory #2, April 19, 2002.
678 Bugtraq, May 14, 2002.
679 Securiteam February 15, 2002.
680 Bugtraq, May 28, 2002.
681 Bugtraq, February 26, 2002.
682 Bugtraq, April 24, 2002.
683 EyeonSecurity, June 5, 2002.
684 SecurityFocus, December 9, 2002.
685 SecurityFocus, December 9, 2002.
686 Bugtraq, August 19, 2002.
687 Bugtraq, June 14, 2002.
688 Securiteam, August 5, 2002.
689 SecurityFocus, July 15, 2002.
690 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:048-06, March 20, 2002.
691 Bugtraq, November 11, 2002.
692 Bugtraq, March 15, 2002.
693 SecurityFocus, September 3, 2002.
694 Bugtraq, January 9, 2002.
695 Securiteam, February 3, 2002.
696 Gentoo Linux Security Announcement, October 1, 2002.
697 Hewlett-Packard Company Security Bulletin, HPSBTL0209-068, October 1, 2002.
698 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:096-24, September 30, 2002.
699 Core Security Technologies Vulnerability Report, CORE-20020620, July 2, 2002.
700 Bugtraq, August 1, 2002.
701 Strumpf Noir Society (SNS) Advisories, February 9, 2002.
702 Bugtraq, April 25, 2002.
703 SecurityFocus, August 6, 2002.
704 Internet Security Systems Security Alert, ISS-109, February 4, 2002.
705 eEye Digital Security Alert, February 8, 2002.
706 NMRC Nomad Mobile Research Centre Advisory, March 20, 2002.
707 Internet Security Systems Security Advisory, April 30, 2002.
708 KPMG-2002019, June 6, 2002.
709 Foundstone Research Labs Advisory, 091802-ISSC, September 18, 2002.
710 Bugtraq, April 11, 2002.
711 SCO Security Advisory, CSSA-2002-038.0, October 24, 2002.
712 Next Generation Security Technologies Security Advisory, NGSEC-2002-2, May 8, 2002.
713 CERT® Advisory CA-2002-12, May 8, 2002.
714 Conectiva Linux Security Announcement, CLA-2002:483, May 9, 2002.
715 FreeBSD Security Notice, FreeBSD-SN-02:02, May 13, 2002.
716 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:105-09, June 4, 2002.
717 Hewlett-Packard Company Security Bulletin, HPSBTL0206-045, June 5, 2002.
718 Conectiva Linux Security Announcement, CLA-2002:494, June 6, 2002.
719 SuSE Security Announcement, SuSE-SA:2002:021, June 6, 2002.
720 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.24, June 10, 2002.
721 CERT® Advisory CA-2002-31, November 14, 2002.
722 Conectiva Linux Security Announcement, CLA-2002:546, November 14, 2002.
723 Debian Security Advisory, DSA 196-1, November 14, 2002.

724 EnGarde Secure Linux Security Advisory, ESA-20021114-029, November 14, 2002.
725 FreeBSD Security Advisory, FreeBSD-SA-02:43, November 14, 2002.
726 Mandrake Linux Security Update Advisory, MDKSA-2002:077, November 14, 2002.
727 SuSE Security Announcement, SuSE-SA:2002:044, November 14, 2002.
728 Bugtraq, September 24, 2002.
729 Bugtraq, November 1, 2002.
730 NGSSoftware Insight Security Research Advisory, NISR09072002, July 9, 2002.
731 Securiteam, January 2, 2002.
732 Foundstone Advisory, FS-052002-21-IPIM, May 20, 2002.
733 Bugtraq, July 30, 2002.
734 @stake, Inc. Security Advisory, a090902-1, August 8, 2002.
735 Securiteam, October 25, 2002.
736 Bugtraq, May 25, 2002.
737 Bugtraq, June 19, 2002.
738 SuSE Security Announcement, SuSE-SA:2002:030, August 12, 2002.
739 Securiteam, August 5, 2002.
740 iDEFENSE Security Advisory, August 28, 2002.
741 Conectiva Linux Security Announcement, CLA-2002:544, November 6, 2002.
742 iDEFENSE Security Advisory, 10.31.02b, October 31, 2002.
743 Bugtraq, January 31, 2002.
744 Securiteam, September 24, 2002.
745 Bugtraq, October 18, 2002.
746 Securiteam, November 21, 2002.
747 SecurityFocus, November 25, 2002.
748 Securiteam, March 16, 2002.
749 Westpoint Security Advisory, wp-02-0011, October 2, 2002.
750 Securiteam, September 30, 2002.
751 Bugtraq, September 28, 2002.
752 Mandrake Linux Security Update Advisory, MDKSA-2002:008, January 22, 2002.
753 SecurityFocus, May 14, 2002.
754 Bugtraq, January 18, 2002.
755 Debian Security Advisory DSA 141-1, August 1, 2002.
756 SecurityFocus, January 8, 2002.
757 NTBugtraq, January 14, 2002.
758 Bugtraq, March 10, 2002.
759 Bugtraq, June 10, 2002.
760 Bugtraq, April 19, 2002.
761 Bugtraq, September 17, 2002.
762 SecurityTracker Alert ID, 1005572, November 8, 2002.
763 Securiteam, December 28, 2001.
764 sp00fed packet advisory #2, September 15, 2002.
765 KDE Security Advisory, September 10, 2002.
766 KDE Security Advisory, October 8, 2002.
767 KDE Security Advisory, November 11, 2002.
768 Mandrake Linux Security Update Advisory, MDKSA-2002:079, November 21, 2002.
769 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:220-40, December 4, 2002.
770 Debian Security Advisory, DSA 204-1, December 5, 2002.
771 KDE Security Advisory, September 10, 2002.
772 Debian Security Advisory, DSA 167-1, September 16, 2002.
773 KDE Security Advisory, November 11, 2002.
774 Gentoo Linux Security Announcement, 200211-004, November 14, 2002.
775 Debian Security Advisory, DSA 193-1, November 11, 2002.
776 SuSE Security Announcement, SuSE-SA:2002:042, November 12, 2002.
777 Securiteam, August 21, 2002.
778 NSSI-Research Labs Security Advisory, NSSI-2002-keriopfw, August 28, 2002.
779 Securiteam, July 7, 2002.
780 Bugtraq, November 13, 2002.
781 Gentoo Linux Security Announcement, 200211-002, November 10, 2002.
782 Securiteam, February 3, 2002.
783 Bugtraq, March 6, 2002.
784 uuappz.com Advisory 002, August 27, 2002.
785 Securiteam, February 3, 2002.
786 SecurityTracker Alert ID 1005376, October 8, 2002.
787 SecurityFocus, April 30, 2002.
788 SecurityFocus, May 14, 2002.
789 Securiteam, July 6, 2002.
790 SecurityTracker Alert ID, 1005764, December 5, 2002.
791 Bugtraq, May 29, 2002.
792 Bugtraq, February 26, 2002.

793 Securiteam, October 21, 2002.
794 Securiteam, April 26, 2002.
795 NetBSD Security Advisory 2002-018, September 17, 2002.
796 SecurityFocus, September 30, 2002.
797 Bugtraq, December 10, 2002.
798 Debian Security Advisory, DSA 152-1, August 13, 2002.
799 SecurityFocus, November 29, 2002.
800 Bugtraq, December 2, 2002.
801 SecurityFocus, November 13, 2002.
802 SCO Security Advisory, CSSA-2002-050.0, November 20, 2002.
803 Conectiva Linux Security Announcement, CLA-2002:491, June 6, 2002.
804 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:094-08, May 29, 2002.
805 Caldera International, Inc. Security Advisory, CSSA-2002-025.0, June 4, 2002.
806 SuSE Security Announcement, SuSE-SA:2002:020, May 29, 2002.
807 Mandrake Linux Security Update Advisory, MDKSA-2002:032, May 16, 2002.
808 Hewlett-Packard Company Security Advisory, HPSBTL0205-044, June 1, 2002.
809 Bugtraq, January 6, 2002.
810 Securiteam, January 16, 2002.
811 Bugtraq, December 23, 2001.
812 Bugtraq, August 13, 2002.
813 DownBload Security Research Lab Advisory, June 28, 2002.
814 Bugtraq, May 14, 2002.
815 Securiteam, May 1, 2002.
816 Securiteam, August 21, 2002.
817 Bugtraq, August 21, 2002.
818 INetCop Security Advisory, 2002-0x82-007, November 27, 2002.
819 Debian Security Advisory, DSA 140-2, August 5, 2002.
820 SCO Security Advisory, CSSA-2002-042.0, November 12, 2002.
821 Bugtraq, February 6, 2002.
822 TESO Security Advisory, January 9, 2002.
823 INetCop Security Advisory, 2002-0x82-002, November 12, 2002.
824 Bugtraq, January 6, 2002.
825 Bugtraq, March 8, 2002.
826 Securiteam, June 9, 2002.
827 enZo Notice, October 24, 2002.
828 iDEFENSE Security Advisory, 11.19.02a, November 19, 2002.
829 CORE Security Technologies, CORE-20021005, December 3, 2002.
830 iDEFENSE Security Advisory, 10.31.02a, November 6, 2002.
831 Securiteam, November 22, 2002.
832 Securiteam, March 22, 2002.
833 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:158-09, August 20, 2002.
834 ALPER Research Labs Security Advisory, ARL02-A09, March 15, 2002.
835 SecurityFocus, April 29, 2002
836 Bugtraq, May 24, 2002.
837 Bugtraq, June 4, 2002.
838 Bugtraq, May 2, 2002.
839 Bugtraq, October 4, 2002.
840 Bugtraq, March 27, 2002.
841 Red Hat Security Advisory, RHSA-2002:054-09, April 4, 2002.
842 SecurityFocus, June 10, 2002.
843 INetCop Security Advisory, 2002-0x82-004, November 16, 2002.
844 KPMG-2002004, February 4, 2002.
845 Securiteam, February 4, 2002.
846 KPMG-2002004, February 4, 2002.
847 Digisec.org Security Advisory, July 2, 2002.
848 Bugtraq, November 7, 2002.
849 Hologram Security Advisory, H20020304, March 4, 2002.
850 Securiteam, July 30, 2002.
851 Securiteam, July 28, 2002.
852 Phenoelit Advisory, July 27, 2002.
853 SecurityFocus, April 30, 2002.
854 ALPER Research Labs Security Advisory, ARL02-A15, June 10, 2002.
855 Bugtraq, June 14, 2002.
856 Securiteam, September 16, 2002.
857 ITCP Advisory 14, May 8, 2002.
858 Bugtraq, March 19, 2002.
859 Bugtraq, May 2, 2002.
860 SecurityFocus, May 10, 2002.
861 Vulnwatch, June 11, 2002.

862 Macromedia Security Bulletin, MPSB02-05, June 27, 2002.
863 Westpoint Security Advisory, WP-02-0009, June 28, 2002.
864 KPMG-2002026, July 1, 2002.
865 KPMG-2002028, July 1, 2002.
866 KPMG-2002032, July 17, 2002.
867 eEye Digital Security Advisory, August 8, 2002.
868 CNET News.com, August 12, 2002.
869 Macromedia Advisory, MPSB02-10, August 8, 2002.
870 Bugtraq, August 11, 2002.
871 Bugtraq, October 7, 2002.
872 Bugtraq, November 18, 2002.
873 Macromedia Advisory, MPSB02-14, December 11, 2002.
874 NGSSoftware Insight Security Research Advisory, NISR29052002, May 29, 2002.
875 Macromedia Security Bulletin, MPSB02-13, November 6, 2002.
876 Macromedia Security Bulletin, MPSB02-12, November 6, 2002.
877 Macromedia Security Bulletin, MPSB02-12, November 6, 2002.
878 Macromedia Security Bulletin, MPSB02-12, November 6, 2002.
879 Securiteam, November 21, 2002.
880 SCAN Associates Advisory, October 28, 2002.
881 Mandrake Linux Security Update Advisory, MDKSA-2002:001, January 9, 2002.
882 Bugtraq, June 17, 2002.
883 Mantis Advisory, 2002-01, August 19, 2002.
884 Mantis Advisory, 2002-04, August 19, 2002.
885 Mantis Advisory, 2002-03, August 19, 2002.
886 Mantis Advisory, 2002-02, August 19, 2002.
887 Mantis Advisory, 2002-05, August 19, 2002.
888 Mantis Advisory, 2002-06, August 23, 2002.
889 Mantis Advisory, 2002-07, August 23, 2002.
890 SecurityFocus, June 10, 2002.
891 Bugtraq, December 15, 2001.
892 Itcp Advisory 3, March 10, 2002.
893 Securiteam, July 7, 2002.
894 KALIF Research Group, October 21, 2002.
895 Securiteam, December 25, 2001.
896 Bugtraq, October 22, 2002.
897 Securiteam, January 20, 2002.
898 Debian Security Advisory, DSA 194-1, November 12, 2002.
899 Strategic Reconnaissance Team Security Advisory, SRT2002-04-31-1159, May 31, 2002.
900 Debian Security Advisory, DSA 116-1, March 2, 2002.
901 Bugtraq, January 23, 2002.
902 INTEXXIA(c) Security Advisory, #1053-040602, June 6, 2002.
903 INTEXXIA(c) Security Advisory, #1054-040602, June 12, 2002.
904 Bugtraq, April 22, 2002.
905 Bugtraq, May 22, 2002.
906 WhiteHat Security Advisory 1004, November 11, 2002.
907 SecurityFocus, May 20, 2002.
908 Securiteam, January 17, 2002.
909 Securiteam, January 20, 2002.
910 SecurityOffice Advisories, September 25, 2002.
911 Bugtraq, April 14, 2002.
912 ISS Security Alert Summary, AS02-10, March 11, 2002.
913 SecurityFocus, April 30, 2002.
914 Bugtraq, June 18, 2002.
915 Securiteam, May 28, 2002.
916 Bugtraq, June 14, 2002.
917 Bugtraq, April 18, 2002.
918 Debian Security Advisory, DSA 199-1, November 19, 2002.
919 Bugtraq, July 24, 2002.
920 Debian Security Advisory, DSA 186-1, November 1, 2002.
921 VulnWatch, January 5, 2002.
922 Bugtraq, October 2, 2002.
923 SecurityFocus, December 20, 2001.
924 Bugtraq, December 20, 2001.
925 Bugtraq, January 3, 2002.
926 Securiteam, December 20, 2001.
927 SecurityFocus, December 21, 2001.
928 Georgi Guninski Security Advisory #52, January 1, 2002.
929 SecurityFocus, January 7, 2002.
930 Bugtraq, December 15, 2001.

931 Microsoft Security Bulletin, MS01-060, December 20, 2001.
932 Microsoft Security Bulletin, MS01-059, December 20, 2001.
933 Securiteam, December 22, 2001.
934 Securiteam, December 21, 2001.
935 Securiteam, January 16, 2002.
936 Bugtraq, January 15, 2002.
937 Bugtraq, January 13, 2002.
938 Jeffrey Dronenburg Advisory, #01-2002, January 15, 2002.
939 Bugtraq, January 22, 2002.
940 Bugtraq, January 21, 2002.
941 Strumpf Noir Society Advisories, January 12, 2002.
942 SecurityFocus, January 23, 2002.
943 Microsoft Security Bulletin, MS02-003, February 7, 2002.
944 Bugtraq, January 31, 2002.
945 Microsoft Security Bulletin, MS02-004, February 7, 2002.
946 Bugtraq, February 2, 2002.
947 Microsoft Security Bulletin, MS02-002, February 6, 2002.
948 RFP2201 Advisory, January 31, 2002.
949 Microsoft Security Bulletin, MS02-001, January 30, 2002.
950 Microsoft Security Bulletin, MS02-001 V1.1, April 24, 2002.
951 SecurityFocus, January 30, 2002.
952 Microsoft Security Bulletin, MS02-010, February 21, 2002.
953 Microsoft Security Bulletin, MS02-005, February 11, 2002.
954 Microsoft Security Bulletin, MS02-009, February 21, 2002.
955 Microsoft Security Bulletin, MS02-009 (Version 1.1), March 13, 2002.
956 Microsoft Security Bulletin, MS02-008, February 21, 2002.
957 Bugtraq, February 12, 2002.
958 Microsoft Security Bulletin, MS02-007, February 21, 2002.
959 NTBugtraq, February 11, 2002.
960 Microsoft Security Bulletin, MS02-006, February 15, 2002.
961 Microsoft Security Bulletin, MS02-006 (version 3.0), March 5, 2002.
962 Microsoft Security Bulletin, MS02-006 (version 4.0), March 11, 2002.
963 Microsoft Security Bulletin, MS02-006 (version 5.0), March 14, 2002.
964 Microsoft Security Bulletin, MS02-006 V6.0, April 26, 2002.
965 Microsoft Security Bulletin, MS02-013, March 4, 2002.
966 Microsoft Security Bulletin, MS02-013 (Version 2.0), March 18, 2002.
967 Microsoft Security Bulletin, MS02-012, February 27, 2002.
968 Microsoft Security Bulletin, MS02-012 (Version 2.0), March 12, 2002.
969 Microsoft Security Bulletin, MS02-011, February 27, 2002.
970 Microsoft Security Bulletin, MS02-011 (Version 2.0), March 12, 2002.
971 NGSSoftware Insight Security Research Advisory, NISR04032002C, March 5, 2002.
972 NTBugtraq, March 7, 2002.
973 Microsoft Security Bulletin, MS02-014, March 7, 2002.
974 Securiteam, March 9, 2002.
975 Bugtraq, March 19, 2002.
976 Bugtraq, March 20, 2002.
977 NTBugtraq, March 14, 2002.
978 Microsoft Security Bulletin, MS02-024, May 22, 2002
979 NTBugtraq, March 26, 2002.
980 GreyMagic Security Advisory, GM#003-IE, March 27, 2002.
981 GreyMagic Security Advisory GM#004-IE, April 2, 2002.
982 Microsoft Security Bulletin, MS02-015, March 28, 2002.
983 Microsoft Security Bulletin, MS02-015 V1.1, April 8, 2002.
984 NTBugtraq, March 28, 2002.
985 Georgi Guninski Security Advisory #53 Version 2.0, April 3, 2002.
986 Georgi Guninski Security Advisory #53 Version 3.0, April 28, 2002.
987 BindView Security Advisory, April 2, 2002.
988 Microsoft Security Bulletin, MS02-016, April 4, 2002.
989 Microsoft Security Bulletin, MS02-016, April 8, 2002.
990 Microsoft Security Bulletin, MS02-017, April 4, 2002.
991 Microsoft Security Bulletin, MS02-017 V1.1, April 16, 2002.
992 NGSSoftware Insight Security Research Advisory, NISR17042002A, April 17, 2002.
993 Bugtraq, April 16, 2002.
994 Bugtraq, April 8, 2002.
995 Thor Larholm Security Advisory, TL#002, April 16, 2002.
996 Bugtraq, April 14, 2002.
997 Securiteam, April 16, 2002.
998 Microsoft Security Bulletin, MS02-019, April 16, 2002.
999 GreyMagic Security Advisory, GM#007-IE, April 8, 2002.

1000 Microsoft Security Bulletin, MS02-044 V1.1, August 22, 2002.
1001 GreyMagic Security Advisory, GM#006-IE, April 8, 2002.
1002 Microsoft Security Bulletin, MS02-044 V1.1, August 22, 2002.
1003 GreyMagic Security Advisory, GM#008-IE, April 8, 2002.
1004 Microsoft Security Bulletin, MS02-044 V1.1, August 22, 2002.
1005 GreyMagic Security Advisory, GM#005-IE, April 8, 2002.
1006 Microsoft Security Bulletin, MS02-044 V1.1, August 22, 2002.
1007 Microsoft Security Bulletin, MS02-020, April 17, 2002.
1008 KPMG-2002011, April 17, 2002.
1009 Securiteam, April 10, 2002.
1010 Finjan Software Security Advisory, April 24, 2002.
1011 Bugtraq, April 24, 2002.
1012 Securiteam, April 20, 2002.
1013 Bugtraq, April 30, 2002.
1014 Microsoft Security Bulletin, MS02-021, April 25, 2002.
1015 Microsoft Security Bulletin MS02-023, May 15, 2002.
1016 Microsoft Security Bulletin, MS02-022, May 8, 2002.
1017 Microsoft Security Bulletin, MS02-022 V2.0, June 11, 2002.
1018 Bugtraq, May 6, 2002.
1019 Georgi Guninski Security Advisory #55, May 24, 2002.
1020 Microsoft Security Bulletin, MS02-025, May 29, 2002.
1021 NTBugtraq, May 23, 2002.
1022 Bugtraq, May 23, 2002.
1023 Bugtraq, May 23, 2002.
1024 Microsoft Security Bulletin, MS02-026 Ver 2.0, June 7, 2002.
1025 Microsoft Security Bulletin, MS02-028, June 12, 2002.
1026 Microsoft Security Bulletin, MS02-028 V2.0, July 1, 2002.
1027 Microsoft Security Bulletin, MS02-027 V2.0, June 14, 2002.
1028 Microsoft Security Bulletin, MS02-047, August 22, 2002.
1029 Bugtraq, June 7, 2002.
1030 Microsoft Security Bulletin, MS02-030, June 12, 2002.
1031 Microsoft, June 13, 2002.
1032 Microsoft Security Bulletin, MS02-029, June 12, 2002.
1033 Microsoft Security Bulletin, MS02-029 V2.0, July 2, 2002.
1034 Microsoft Security Bulletin, MS02-033, June 26, 2002.
1035 Microsoft Security Bulletin MS02-031, June 19, 2002.
1036 Securiteam, June 17, 2002.
1037 NGSSoftware Insight Security Research Advisory, NISR19062002, June 19, 2002.
1038 Securiteam, June 15, 2002.
1039 Microsoft Security Bulletin, MS02-032, June 26, 2002.
1040 Microsoft Security Bulletin MS02-032 V2.0, July 24, 2002.
1041 Thor Larholm, PivX, Security Advisory, TL#003, July 10, 2002.
1042 Microsoft Security Bulletin, MS02-047, August 22, 2002.
1043 Microsoft Security Bulletin, MS02-034, July 10, 2002.
1044 Microsoft Security Bulletin, MS02-035, July 10, 2002.
1045 Portcullis Security Advisory, July 12, 2002.
1046 Microsoft Security Bulletin, MS02-037, July 24, 2002.
1047 Microsoft Security Bulletin, MS02-036, July 24, 2002.
1048 Bugtraq, July 19, 2002.
1049 SecurityFocus, July 20, 2002.
1050 Microsoft Security Bulletin, MS02-038, July 24, 2002.
1051 Microsoft Security Bulletin, MS02-039, July 24, 2002.
1052 SecurityFocus, July 17, 2002.
1053 Microsoft Security Bulletin, MS02-041, August 7, 2002.
1054 Bugtraq, August 6, 2002.
1055 Bugtraq, August 6, 2002.
1056 Bugtraq, August 5, 2002.
1057 Georgi Guninski Security Advisory #57, July 31, 2002.
1058 Microsoft Security Bulletin, MS02-040, July 31, 2002.
1059 NTBugtraq, July 27, 2002.
1060 Bugtraq, August 6, 2002.
1061 Bugtraq, August 5, 2002.
1062 Bugtraq, August 6, 2002.
1063 Microsoft Security Bulletin, MS02-071, December 11, 2002.
1064 Securiteam, August 1, 2002.
1065 Bugtraq, July 30, 2002.
1066 @stake Inc. Security Advisory, A081602-1, August 16, 2002.
1067 Microsoft Security Bulletin, MS02-042, August 14, 2002.
1068 NGSSoftware Insight Security Research Advisory, #NISR15002002B, August 15, 2002.

1069 Microsoft Security Bulletin, MS02-043, August 14, 2002.
1070 Bugtraq, August 16, 2002.
1071 Bugtraq, August 18, 2002.
1072 Securiteam, August 19, 2002.
1073 NTBugtraq, August 15, 2002.
1074 Microsoft Security Bulletin, MS02-047, August 22, 2002.
1075 Bugtraq, August 13, 2002.
1076 Bugtraq, August 17, 2002.
1077 Microsoft Security Bulletin, MS02-046, August 22, 2002.
1078 Bugtraq, August 21, 2002.
1079 Microsoft Security Bulletin, MS02-045, August 22, 2002.
1080 Bugtraq, August 15, 2002.
1081 Microsoft Security Bulletin, MS02-060 V1.1, October 17, 2002.
1082 Bugtraq, September 3, 2002.
1083 NGSSoftware Insight Security Research Advisory, NISR03092002A, September 3, 2002.
1084 Microsoft Security Bulletin, MS02-049, September 4, 2002.
1085 Microsoft Security Bulletin, MS02-048, August 28, 2002.
1086 Microsoft Security Bulletin, MS02-050 V2.2, September 5, 2002.
1087 Microsoft Security Bulletin, MS02-050 V4.0, November 20, 2002.
1088 Bugtraq, August 26, 2002.
1089 Microsoft Security Bulletin, MS02-059 V1.1, October 17, 2002.
1090 GreyMagic Security Advisory, GM#010-IE, September 9, 2002.
1091 Bugtraq, September 9, 2002.
1092 Securiteam, September 18, 2002.
1093 Bugtraq, September 9, 2002.
1094 Microsoft Security Bulletin, MS02-052, September 18, 2002.
1095 Microsoft Security Bulletin, MS02-051, September 18, 2002.
1096 Abtrusion Security, September 18, 2002.
1097 Microsoft Security Bulletin, MS02-056, October 2, 2002.
1098 Microsoft Security Bulletin MS02-053 V1.1, September 26, 2002
1099 Bugtraq, October 1, 2002.
1100 SecurityFocus, September 17, 2002
1101 Bugtraq, September 23, 2002.
1102 Microsoft Security Bulletin, MS02-057, October 2, 2002.
1103 SecurityFocus, September 23, 2002.
1104 phion Security Advisory, September 26, 2002.
1105 Microsoft Security Bulletin, MS02-055, October 2, 2002.
1106 Microsoft Security Bulletin, MS02-054, October 2, 2002.
1107 Bugtraq, September 19, 2002.
1108 Bugtraq, October 7, 2002.
1109 Microsoft Security Bulletin, MS02-061, October 16, 2002.
1110 SecurityFocus, October 5, 2002.
1111 Bugtraq, October 7, 2002.
1112 GreyMagic Security Advisory, GM#011-IE, October 15, 2002.
1113 Microsoft Security Bulletin, MS02-058 V1.2, October 11, 2002.
1114 SNS Advisory No.56, October 11, 2002.
1115 Securiteam, October 17, 2002.
1116 Security Advisory 10.06.2002, October 9, 2002.
1117 Bugtraq, October 4, 2002.
1118 Microsoft Security Bulletin, MS02-063, October 30, 2002.
1119 Bugtraq, October 21, 2002.
1120 GreyMagic Security Advisory GM#012-IE, October 22, 2002.
1121 Microsoft Security Bulletin, MS02-062, October 30, 2002.
1122 Securiteam, October 22, 2002.
1123 Microsoft Security Bulletin, MS02-064, October 30, 2002.
1124 Immunity Inc. Advisory, October 18, 2002.
1125 Bugtraq, October 18, 2002.
1126 Bugtraq, November 8, 2002.
1127 NTBugtraq, November 2, 2002.
1128 Bugtraq, November 9, 2002.
1129 Microsoft Security Bulletin, MS02-065 V1.1, November 22, 2002.
1130 Microsoft Security Bulletin, MS02-066 V1.1, November 25, 2002.
1131 Bugtraq, November 20, 2002.
1132 Microsoft Security Bulletin, MS02-069, December 11, 2002.
1133 Microsoft Security Bulletin, MS02-068 V2.0, December 6, 2002.
1134 Microsoft Security Bulletin, MS02-067, December 4, 2002.
1135 Microsoft Security Bulletin, MS02-070, December 11, 2002.
1136 Microsoft Security Bulletin, MS02-071, December 11, 2002.
1137 Securiteam, December 1, 2002.

1138 SNS Advisory No.60, December 5, 2002.
1139 Bugtraq, December 3, 2002.
1140 Microsoft Security Bulletin, MS02-018 V1.2, April 12, 2002.
1141 Cisco Advisory, CI-02.04, April 15, 2002.
1142 Microsoft Security Bulletin, MS02-018 V1.3, May 6, 2002.
1143 SecurityFocus, April 29, 2002.
1144 SecurityFocus, January 8, 2002.
1145 Bugtraq, February 5, 2002.
1146 Bugtraq, April 14, 2002.
1147 Bugtraq, July 15, 2002.
1148 Bugtraq, July 24, 2002.
1149 Bugtraq, May 24, 2002.
1150 Bugtraq, June 14, 2002.
1151 Qitest1 Security Advisory #003, May 11, 2002.
1152 Securiteam, December 1, 2002.
1153 Bugtraq, June 24, 2002.
1154 Trustix Secure Linux Security Advisory, TSL-2002-0058, June 28, 2002.
1155 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.32, July 1, 2002.
1156 EnGarde Secure Linux Security Advisory, ESA-20020702-017, July 2, 2002.
1157 Conectiva Linux Security Announcement, CLA-2002:504, July 2, 2002.
1158 Securiteam, October 25, 2002.
1159 Securiteam, December 11, 2002.
1160 Bugtraq, December 9, 2002.
1161 Bugtraq, October 10, 2002.
1162 Illegal Instruction Labs Advisory, September 25, 2002.
1163 Illegal Instruction Labs Advisory, September 30, 2002.
1164 Securiteam, November 7, 2002.
1165 Bugtraq, April 23, 2002.
1166 Bugtraq, April 23, 2002.
1167 Sandblad advisory #9, July 24, 2002.
1168 SecurityFocus, December 28, 2001.
1169 SecurityFocus, January 8, 2002.
1170 SecurityFocus, January 8, 2002.
1171 Bugzilla Security Advisory, June 8, 2002.
1172 SecurityFocus, August 6, 2002.
1173 Bugtraq, August 19, 2002.
1174 Securiteam, September 12, 2002.
1175 Bugzilla Security Advisory, October 1, 2002.
1176 Bugtraq, September 18, 2002.
1177 Bugzilla Security Advisory, November 26, 2002.
1178 GreyMagic Security Advisory, GM#001-NS, April 30, 2002.
1179 Bugtraq, May 12, 2002.
1180 Bugtraq, November 14, 2002.
1181 Bugtraq, November 26, 2002.
1182 UKR Security Team Advisory, February 2, 2002.
1183 Bugtraq, February 4, 2002.
1184 Gobbles Security Advisory, December 18, 2001.
1185 SecurityFocus, January 7, 2002.
1186 Bugtraq, January 2, 2002.
1187 KSSA-003, January 20, 2002.
1188 Strumpf Noir Society Summaries, January 21, 2002.
1189 Strumpf Noir Society Summaries, January 21, 2002.
1190 Nomad Mobile Research Centre Advisory, January 14, 2002.
1191 Bugtraq, January 21, 2002.
1192 Bugtraq, January 10, 2002.
1193 SecurityFocus, February 19, 2002.
1194 SecurityFocus, February 19, 2002.
1195 CERT® Advisory CA-2002-03, February 12, 2002.
1196 Hewlett-Packard Company Security Bulletin, HPSBMP0206-015, June 17, 2002.
1197 SecurityFocus, February 23, 2002.
1198 CERT® Advisory CA-2002-06, March 4, 2002.
1199 Bugtraq, February 27, 2002.
1200 Bugtraq, March 6, 2002.
1201 Bugtraq, February 19, 2002.
1202 nCipher Security Advisory #2, February 27, 2002.
1203 Bugtraq, March 19, 2002.
1204 Bugtraq, March 18, 2002.
1205 Securiteam, March 26, 2002.
1206 BindView Security Advisory, April 8, 2002.

1207 FreeBSD Security Advisory, FreeBSD-SA-02:23, April 22, 2002.
1208 Bugtraq, April 30, 2002.
1209 Core Security Technologies Advisory, CORE-20020409, April 24, 2002.
1210 Bugtraq, May 10, 2002.
1211 SecurityFocus, May 11, 2002.
1212 Bugtraq, June 14, 2002.
1213 Westpoint Security Advisory, wp-02-0002, June 28, 2002.
1214 Bugtraq, July 7, 2002.
1215 PTrace Networks Security, June 28, 2002.
1216 Bugtraq, July 11, 2002.
1217 asciiSECURE Advisory, July 17, 2002.
1218 asciiSECURE Advisory, July 17, 2002.
1219 Sandblad Advisory #8, July 23, 2002.
1220 Bugtraq, July 23, 2002.
1221 iDEFENSE Security Advisory, 08.08.2002.
1222 XWT Foundation Security Advisory, July 29, 2002.
1223 Bugtraq, August 20, 2002.
1224 Foundstone Labs Advisory, 080902-APIL, August 9, 2002.
1225 Debian Security Advisory, DSA 154-1, August 15, 2002.
1226 Bugtraq, August 12, 2002.
1227 Securiteam, September 12, 2002.
1228 Securiteam, September 8, 2002.
1229 Rapid 7, Inc. Security Advisory, October 3, 2002.
1230 Hewlett-Packard Company Security Bulletin, HPSBUX0209-222, September 30, 2002.
1231 Hewlett Packard Systems Security Bulletin, SSRT2368, October 7, 2002.
1232 Bugtraq, October 10, 2002.
1233 Hewlett-Packard Company Security Bulletin, HPSBUX0210-224, October 30, 2002.
1234 NetBSD Security Advisory, 2002-016, October 22, 2002.
1235 SecurityFocus, October 21, 2002.
1236 SecurityFocus, November 1, 2002.
1237 Bugtraq, November 11, 2002.
1238 ISS X-Force Security Brief, November 25, 2002.
1239 SGI Security Advisory, 20021202-01-I, December 4, 2002.
1240 Hewlett-Packard Company Security Bulletin, HPSBUX0212-228, December 6, 2002.
1241 Sun(sm) Alert Notification, 48879, November 25, 2002.
1242 SGI Security Advisory, 20021205-01-A, December 13, 2002.
1243 iDEFENSE Security Advisor, 10.03.2002, October 3, 2002.
1244 OpenPKG Security Advisory, OpenPKG-SA-2002.009, October 4, 2002.
1245 EnGarde Secure Linux Security Advisory, ESA-20021007-024, October 7, 2002.
1246 FreeBSD Security Notice, FreeBSD-SN-02:06, October 10, 2002.
1247 Mandrake Linux Security Update Advisory, MDKSA-2002:068, October 16, 2002.
1248 Oracle Security Alert #45, October 4, 2002.
1249 Trustix Secure Linux Security Advisory, 2002-0069, October 17, 2002.
1250 SecurityFocus, October 30, 2002.
1251 Hewlett-Packard Company Security Bulletin, HPSBUX0210-224, October 30, 2002.
1252 Debian Security Advisory, DSA 187-1, November 4, 2002.
1253 Debian Security Advisory, DSA 188-1, November 5, 2002.
1254 SGI Security Advisory, 20021105-01-I, November 12, 2002.
1255 Debian Security Advisory, DSA 195-1, November 13, 2002.
1256 Gentoo Linux Security Announcement, 200211-003, November 12, 2002.
1257 SCO Security Advisory, CSSA-2002-056.0, December 5, 2002.
1258 Hewlett Packard Systems Security Bulletin, HPSBTL0210-073, October 15, 2002.
1259 RedHat Security Advisory, RHSA-2002:194-18, October 10, 2002.
1260 Debian Security Advisory DSA 207-1, December 11, 2002.
1261 Conectiva Linux Security Announcement, CLA-2002:464, February 27, 2002.
1262 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.7, March 4, 2002.
1263 SuSE Security Announcement, SuSE-SA:2002:008, March 5, 2002.
1264 NetBSD Security Advisory, 2002-026, October 21, 2002.
1265 Gentoo Linux Security Announcement, 200210-008, October 26, 2002.
1266 Debian Security Advisory, DSA 183-1, October 29, 2002.
1267 Debian Security Advisory, DSA 184-1, October 30, 2002.
1268 Mandrake Linux Security Update Advisory, MDKSA-2002:073, October 29, 2002.
1269 MIT krb5 Security Advisory, MITKRB5-SA-2002-, October 26, 2002.
1270 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:242-06, November 7, 2002.
1271 Debian Security Advisory, DSA 180-1, October 21, 2002.
1272 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:223-07, October 24, 2002.
1273 Hewlett Packard Security Bulletin, HPSBTL0210-074, October 26, 2002.
1274 Gentoo Linux Security Announcement, 200210-010, October 28, 2002.
1275 Conectiva Linux Security Announcement, CLA-2002:539, November 6, 2002.

1276 EnGarde Secure Linux Security Advisory, ESA-20021029-027, October 29, 2002.
1277 Debian Security Advisory, DSA 181-1, October 22, 2002.
1278 OpenPKG Security Advisory, OpenPKG-SA-2002.010, October 23, 2002.
1279 Mandrake Linux Security Update Advisory, MDKSA-2002:072, October 24, 2002.
1280 Gentoo Linux Security Announcement, 200210-009, October 27, 2002.
1281 Conectiva Linux Security Announcement, CLA-2002:541, November 6, 2002.
1282 NetBSD Security Advisory, 2002-001, January 16, 2002.
1283 FreeBSD Security Advisory, FreeBSD-SA-02:08, January 24, 2002.
1284 Debian Security Advisor, DSA 110-1, February 13, 2002.
1285 Mandrake Linux Security Update Advisory, MDKSA-2002:015, February 15, 2002.
1286 Bugtraq, February 27, 2002.
1287 Red Hat Security Advisory, Rhsa-2002:028-13, February 27, 2002.
1288 Sun Microsystems, Inc. Security Bulletin, Sun-00218, March 18, 2002.
1289 Hewlett-Packard Company Security Bulletin, HPSBUX0203-187, March 19, 2002.
1290 Sun Microsystems, Inc. Security Bulletin, #00217, March 18, 2002.
1291 Hewlett-Packard Company Security Bulletin, HPSBUX0203-188, March 19, 2002.
1292 eSecurityOnline Security Advisory 2406, April 29, 2002.
1293 Compaq Computer Corporation Security Bulletin, SSRT-541, April 18, 2002.
1294 Cartel Sécurité Security Advisory, CARTSA-20020402, May 8, 2002.
1295 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:086-05, May 9, 2002.
1296 OpenBSD Security Advisory, June 27, 2002.
1297 FreeBSD Security Advisory, FreeBSD-SA-02:30, July 12, 2002.
1298 RUS-CERT Advisory 2002-08:02, August 5, 2002.
1299 Debian Security Advisory, DSA 146-1, August 8, 2002.
1300 FreeBSD Security Advisory, FreeBSD-SA-02:32, July 31, 2002.
1301 NetBSD Security Advisory 2002-010, August 2, 2002.
1302 Intercept Ricochet Advisory, August 12, 2002.
1303 CERT® Advisory, CA-2002-26, August 12, 2002.
1304 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:210-06, October 17, 2002.
1305 Trustix Secure Linux Security Advisory, TSLSA-2002-0068, October 17, 2002.
1306 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:206-12, October 15, 2002.
1307 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:205-15, October 17, 2002.
1308 SuSE Security Announcement, SuSE-SA:2002:037, October 14, 2002.
1309 Debian Security Advisory, DSA 174-1, October 14, 2002
1310 CERT/CC Vulnerability Note VU#266817, November 4, 2002.
1311 SGI Security Advisory, 20021103-01-P, November 8, 2002.
1312 CERT® Advisory CA-2002-31, November 14, 2002.
1313 OpenPKG Security Advisory, OpenPKG-SA-2002.011, November 15, 2002.
1314 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:132-14, July 29, 2002.
1315 Trustix Secure Linux Security Advisory, TSLSA-2002-0064, July 30, 2002.
1316 Hewlett-Packard Company Security, HPSBTL0207-054, July 30, 2002.
1317 SCO Security Advisory, CSSA-2002-043.0, October 29, 2002.
1318 Pine Internet Security Advisory, 20020601, June 25, 2002.
1319 NetBSD Security Advisory, 2002-006, June 27, 2002.
1320 FreeBSD Security Advisory, FreeBSD-SA-02:28, June 26, 2002.
1321 Core Security Technologies, CORE-20020528, July 10, 2002.
1322 CERT® Advisory, CA-2002-20, July 11, 2002.
1323 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.28, July 11, 2002.
1324 SuSE Security Announcement, SuSE-SA:2002:041, November 5, 2002.
1325 Gentoo Linux Security Announcement, 200211-001, November 6, 2002.
1326 Mandrake Linux Security Update Advisory, MDKSA-2002:076, November 7, 2002.
1327 SuSE Security Announcement, SuSE-SA:2002:003, January 16, 2002.
1328 Debian Security Advisory, DSA 102-2, January 18, 2002.
1329 Mandrake Linux Security Update Advisory, MDKSA-2002:007, January 18, 2002.
1330 Red Hat Security Advisory, RHSA-2002:015-13, January 22, 2002.
1331 Trustix Secure Linux Security Advisory, 2002-0034, February 28, 2002.
1332 EnGarde Secure Linux Security Advisory, ESA-20020301-005, March 1, 2002.
1333 Conectiva Linux Security Announcement, CLA-2002:465, March 4, 2002.
1334 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:153-07, July 30, 2002.
1335 Mandrake Linux Security Update Advisory, MDKSA-2002:045, July 29, 2002.
1336 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:153-07, July 30, 2002.
1337 SuSE Security Announcement, SuSE-SA:2002:028, July 31, 2002.
1338 Hewlett Packard Systems Security Bulletin, SSRT2339, October 7, 2002.
1339 SCO Security Advisory, CSSA-2002-SCO.40, October 10, 2002.
1340 Sun(sm) Alert Notification 47903, October 15, 2002.
1341 IBM Alert, October 11, 2002.
1342 NetBSD Security Advisory 2002-015, October 8, 2002.
1343 Conectiva Linux Security Announcement, CLA-2002:535, November 6, 2002.
1344 FreeBSD Security Advisory, FreeBSD-SA-02:42, November 13, 2002.

1345 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:197-09, November 7, 2002.
1346 Red Hat Security Advisory, RHSA-2001:160-09, December 14, 2001.
1347 Conectiva Linux Security Announcement, CLA-2002:447, January 3, 2001.
1348 EnGarde Secure Linux Security Advisory, ESA-20011217-01, December 17, 2001.
1349 Trustix Secure Linux Security Advisory, TSLSA-2001-0029, December 19, 2001.
1350 Hewlett-Packard Company Security Bulletin, HPSBTL0112-008, December 17, 2001.
1351 Mandrake Linux Security Update Advisory, MDKSA-2001:095, December 19, 2001.
1352 SuSE Security Announcement, SuSE-SA:2002:004, January 25, 2002.
1353 Conectiva Linux Security Announcement, CLA-2002:458, January 25, 2002.
1354 EnGarde Secure Linux Security Advisory, ESA-20020125-004, January 25, 2002.
1355 Debian Security Advisory, DSA-106-1, January 26, 2002.
1356 Mandrake Linux Security Update Advisory, MDKSA-2002:009, January 28, 2002.
1357 Trustix Secure Linux Security Advisory, 2002-0025, January 28, 2002.
1358 Red Hat Security Advisory, RHSA-2002:018-10, January 30, 2002.
1359 Hewlett-Packard Company Security Advisory, HPSBTL0201-022, January 30, 2002.
1360 Red Hat Security Advisory, RHSA-2002:027-22, 2002:026-35 & 39, March 11, 2002.
1361 SuSE Security Announcement, SuSE-SA:2002:010 & 2002:011, March 11, 2002.
1362 EnGarde Secure Linux Security Advisory, ESA-20020311-008, March 11, 2002.
1363 Debian Security Advisory, DSA 122-1, March 11, 2002.
1364 Mandrake Linux Security Update Advisory, MDKSA-2002:022 & MDKSA-2002:023-1, March 12, 2002.
1365 OpenPKG Security Advisory, OpenPKG-SA-2002.003, March 12, 2002.
1366 Conectiva Linux Security Announcement, CLA-2002:469, March 14, 2002.
1367 FreeBSD Security Advisory, FreeBSD-SA-02:18, March 18, 2002.
1368 Trustix Secure Linux Security Advisory, TSLSA-2002-0040, March 18, 2002.
1369 e-matters GmbH Advisory 012002, February 27, 2002.
1370 Mandrake Linux Security Update Advisory, MDKSA-2002:017, February 28, 2002.
1371 RedHat Security Advisory, RHSA-2002:035-13, February 28, 2002.
1372 SuSE Security Announcement, SuSE-SA:2002:007, February 28, 2002.
1373 Trustix Secure Linux Security Advisory, 2002-0033, February 28, 2002.
1374 EnGarde Secure Linux Security Advisory, ESA-20020301-006, March 1, 2002.
1375 Debian Security Advisory, DSA 115-1, March 2, 2002.
1376 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:072-07, April 25, 2002.
1377 Conectiva Linux Security Announcement, CLA-2002:475, April 26, 2002.
1378 Debian Security Advisory, DSA-128-1, April 26, 2002.
1379 Mandrake Linux Security Update Advisory, MDKSA-2002:028, April 26, 2002.
1380 EnGarde Secure Linux Security Advisory, ESA-20020429-010, April 29, 2002.
1381 Trustix Secure Linux Security Advisory, TSLSA-2002-0046, April 29, 2002.
1382 SuSE Security Announcement, SuSE-SA:2002:014, April 30, 2002.
1383 Conectiva Linux Security Announcement, CLA-2002:467, March 7, 2002.
1384 Debian Security Advisory, DSA-119-1, March 8, 2002.
1385 EnGarde Secure Linux Security Advisory, ESA-20020307-007, March 7, 2002.
1386 Mandrake Linux Security Update Advisory, MDKSA-2002:019, March 8, 2002.
1387 Red Hat Security Advisory, RHSA-2002:043-10, March 8, 2002.
1388 SuSE Security Announcement, SuSE-SA:2002:009, March 7, 2002.
1389 OpenPKG Security Advisory, OpenPKG-SA-2002.001, March 8, 2002.
1390 Pine Internet Security Advisory, PINE-CERT-20020301, March 7, 2002.
1391 Internet Security Systems Advisory, July 31, 2002.
1392 SGI Security Advisory, 20020801-01-A, August 1, 2002.
1393 FreeBSD Security Advisory, FreeBSD-SA-02:34 revised, August 1, 2002.
1394 NetBSD Security Advisory, 2002-011, August 2, 2002.
1395 Debian Security Advisory, DSA 142-1, August 5, 2002.
1396 Debian Security Advisory, DSA 143-1, August 5, 2002.
1397 OpenAFS Security Advisory, 2002-001, August 3, 2002.
1398 Apple Security Update, 2002-08-02, August 2, 2002.
1399 CERT Advisory CA-2002-17, June 17, 2002.
1400 SuSE Security Announcement, SuSE-SA:2002:022, June 18, 2002.
1401 EnGarde Secure Linux Security Advisory, ESA-20020619-014, June 19, 2002.
1402 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:103-13, June 19, 2002.
1403 OpenPKG Security Advisory, OpenPKG-SA-2002.004, June 19, 2002.
1404 Debian Security Advisory DSA-131-2, June 19, 2002.
1405 Slackware Security Team, June 19, 2002.
1406 Trustix Secure Linux Security Advisory, TSLSA-2002-0056, June 20, 2002.
1407 Mandrake Linux Security Update Advisory, MDKSA-2002:039-2, June 22, 2002.
1408 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.31, July 1, 2002.
1409 Caldera International, Inc. Security Advisory, CSSA-2002-SCO.32, July 1, 2002.
1410 CERT® Advisory CA-2002-17, updated July 8, 2002.
1411 CERT® Advisory, CA-2002-18, June 25, 2002.
1412 Conectiva Linux Security Announcement, CLA-2002:500, June 25, 2002.
1413 EnGarde Secure Linux Security Advisory, ESA-20020625-015, June 25, 2002.

1414 SuSE Security Announcement, SuSE-SA:2002:023, June 25, 2002.
1415 OpenPKG Security Advisory, OpenPKG-SA-2002.005, June 26, 2002.
1416 NetBSD Security Advisory, 2002-005, June 27, 2002.
1417 Caldera International, Inc. Security Advisory, CSSA-2002-030.0, June 27, 2002.
1418 Debian Security Advisory, DSA-134-4, June 27, 2002.
1419 Mandrake Linux Security Update Advisory, MDKSA-2002:040, June 24, 2002.
1420 Trustix Secure Linux Security Advisory, 2002-0059, June 28, 2002.
1421 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:127-18, June 27, 2002.
1422 Conectiva Linux Security Announcement, CLA-2002:502, June 28, 2002.
1423 Revised OpenSSH Security Advisory, July 2, 2002.
1424 EnGarde Secure Linux Security Advisory, ESA-20020702-016, July 2, 2002.
1425 SuSE Security Announcement, SuSE-SA:2002:024, July 2, 2002.
1426 Mandrake Linux Security Update Advisory, MDKSA-2002:040-1, July 2, 2002.
1427 Securiteam, December 4, 2002.
1428 Debian Security Advisory, DSA-096-1, January 2, 2002.
1429 Debian Security Advisory, DSA-096-2, January 3, 2002.
1430 Trustix Secure Linux Security Advisory #2002-0003, January 4, 2002.
1431 FreeBSD Security Advisory, FreeBSD-SA-02:04, January 6, 2002.
1432 Conectiva Linux Security Announcement, CLA-2002:449, January 7, 2002.
1433 Red Hat Security Advisory, RHSA-2002:003-10, January 7, 2002.
1434 SuSE Security Announcement, SuSE-SA:2002:001, January 7, 2002.
1435 SecurityFocus, June 15, 2002.
1436 SecurityFocus, May 11, 2002.
1437 Bugtraq, October 21, 2002.
1438 Bugtraq, October 16, 2002.
1439 INetCop Security Advisory #2002-0x82-010, December 11, 2002.
1440 SecurityFocus, October 2, 2002.
1441 Bugtraq, August 18, 2002.
1442 Westpoint Security Advisory, wp-02-0003, October 2, 2002.
1443 Foundstone Advisory, FS-070302-24-MWSX, July 8, 2002.
1444 D4rkGr3y Advisory, August 14, 2002.
1445 Securiteam, October 15, 2002.
1446 Red Hat Security Advisory, RHSA-2001:162-04, December 7, 2001.
1447 Bugtraq, April 22, 2002.
1448 Squid Proxy Cache Security Update Advisory, SQUID-2002:2, March 26, 2002.
1449 Squid Security Update Advisory, SQUID-2002:3, July 3, 2002.
1450 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:051-16, July 2, 2002.
1451 Conectiva Linux Security Announcement, CLA-2002:506, July 5, 2002.
1452 SuSE Security Announcement, SuSE-SA:2002:025, July 9, 2002.
1453 Squid Proxy Cache Security Update Advisory, SQUID-2002:1, February 21, 2002.
1454 FreeBSD Security Advisory, FreeBSD-SA-02:12, February 21, 2002.
1455 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:029-09, February 26, 2002.
1456 Mandrake Linux Security Update Advisory, MDKSA-2002:016-1, February 26, 2002.
1457 Conectiva Linux Security Announcement, CLA-2002:464, February 27, 2002.
1458 nCipher Security Advisory #3, May 13, 2002.
1459 nCipher Security Advisory No. 5, August 19, 2002.
1460 nCipher[TM] Security Advisory No. 4, June 17, 2002.
1461 ISS Security Alert Summary, AS02-27, July 8, 2002.
1462 Bugtraq, July 3, 2002.
1463 ISS Security Alert Summary, AS02-27, July 8, 2002.
1464 Bugtraq, November 16, 2002.
1465 Securiteam, April 4, 2002.
1466 NetBSD Security Advisory, 2002-007, September 17, 2002.
1467 NetBSD Security Advisory 2002-012, September 17, 2002.
1468 NetBSD Security Advisory 2002-014, September 17, 2002.
1469 NetBSD Security Advisory, 2002-019, October 8, 2002.
1470 NetBSD Security Advisory, 2002-025, October 24, 2002.
1471 NetBSD Security Advisory, 2002-027, November 19, 2002.
1472 Netfilter Core Team Security Advisory, December 3, 2002.
1473 Bugtraq, January 15, 2002.
1474 Bugtraq, February 3, 2002.
1475 Bugtraq, February 15, 2002.
1476 Bugtraq, September 7, 2002.
1477 Bugtraq, September 27, 2002.
1478 Securiteam October 11, 2002.
1479 Securiteam, October 11, 2002.
1480 Bugtraq, June 17, 2002.
1481 Bugtraq, January 18, 2002.
1482 ISS Security Alert Summary AS02-37, September 16, 2002.

1483 Procheckup Security Bulletin, PR02-1, May 29, 2002.
1484 Infobyte Security Research, June 13, 2002.
1485 Bugtraq, November 20, 2002.
1486 iDEFENSE Security Advisory, 11.19.02c, November 19, 2002.
1487 Bugtraq, November 26, 2002.
1488 CERT Vulnerability Note, VU#191763, January 8, 2002.
1489 CERT Vulnerability Note, VU#985347, January 8, 2002.
1490 GreyMagic Security Advisory, GM#001-NS, April 30, 2002.
1491 Securiteam, May 27, 2002.
1492 SecurityFocus, June 5, 2002.
1493 NetScreen Security Advisory, September 6, 2002.
1494 NetScreen Security Alert 51929, November 25, 2002.
1495 NetScreen Security Alert 51929, November 25, 2002.
1496 NetScreen Security Alert 51897, November 25, 2002.
1497 NetScreen Security Alert 51929, November 25, 2002.
1498 NetScreen Security Alert 52020, November 25, 2002.
1499 NetScreen Security Advisory, January 21, 2002.
1500 Axioma Security Research Advisory, January 3, 2002.
1501 iDEFENSE Security Advisory, 10.02.2002, October 2, 2002.
1502 NGSSoftware Insight Security Research Advisory, NISR18022002, February 19, 2002.
1503 Bugtraq, February 21, 2002.
1504 NGSSoftware Insight Security Research Advisory, NISR12022002, February 13, 2002.
1505 Securiteam, January 8, 2002.
1506 Bugtraq, January 25, 2002.
1507 Bugtraq, May 8, 2002.
1508 eEye Digital Security Advisory, July 10, 2002.
1509 Bugtraq, July 25, 2002.
1510 CERT Vulnerability Note VU#287771, August 11, 2002.
1511 Foundstone Labs Advisory, 090502-PCRO, September 5, 2002.
1512 Bugtraq, November 29, 2002.
1513 Securiteam, January 16, 2002.
1514 Westpoint Security Advisory, wp-02-0006, May 22, 2002.
1515 Securiteam, March 23, 2002.
1516 Bugtraq, July 27, 2002.
1517 Securiteam, February 25, 2002.
1518 ppp-design Advisory, May 14, 2002.
1519 Bugtraq, June 24, 2002.
1520 IRM Security Advisory 002, December 19, 2001.
1521 Bugtraq, February 19, 2002.
1522 Securiteam, January 29, 2002.
1523 Bugtraq, April 12, 2002.
1524 iDEFENSE Security Advisory, 11.04.02b, November 4, 2002.
1525 Bugtraq, December 15, 2001.
1526 Bugtraq, January 31, 2002.
1527 Bugtraq, February 20, 2002.
1528 Bugtraq, February 28, 2002.
1529 iXsecurity Security Vulnerability Report, iXsecurity.20020313, April 2, 2002.
1530 Bugtraq, May 10, 2002.
1531 cquire.net Security Vulnerability Report, 20020412, May 8, 2002.
1532 cquire.net Security Vulnerability Report, 20020408, May 8, 2002.
1533 Bugtraq, May 30, 2002.
1534 cquire.net Security Vulnerability Report, 20020604, June 25, 2002.
1535 cquire.net Security Vulnerability Report, 20020521, June 25, 2002.
1536 Cluestick Advisory #001, June 27, 2002.
1537 Bugtraq, July 25, 2002.
1538 PricewaterhouseCoopers Security Vulnerability Report, pwc.20020630, July 15, 2002.
1539 Security Alert, NOVL-2002-2963297, August 20, 2002.
1540 Security Alert, NOVL- 2002-2963307, August 20, 2002.
1541 Security Alert, NOVL- 2002-2963297, August 20, 2002.
1542 NOVL-2002-2963349, August 21, 2002.
1543 Novell Security Alert,NOVL-2002-2963651, November 11, 2002.
1544 Novell Security Alert, NOVL-2002-2963767, November 12, 2002.
1545 Novell Security Alert, NOVL-2002-2963827, November 12, 2002.
1546 ECHU Alert #2, September 25, 2002.
1547 Bugtraq, September 2, 2002.
1548 Netric Security Advisory, September 22, 2002.
1549 SecurityFocus, November 26, 2002.
1550 Debian Security Advisory, DSA 198-1, November 18, 2002.
1551 Sandblad Advisory #5, April 26, 2002.

1552 Securiteam, May 21, 2002.
1553 Netric Security Team, June 4, 2002.
1554 Security Advisory Número Dos, July 5, 2002.
1555 Bugtraq, July 17, 2002.
1556 Fate Research Laboratories Security Advisory, August 6, 2002.
1557 Illegal Instruction Security Research Labs Advisory, August 4, 2002.
1558 Illegal Instruction Labs Advisory, September 29, 2002.
1559 Bugtraq, January 22, 2002.
1560 Bugtraq, October 10, 2002.
1561 Bugtraq, March 14, 2002.
1562 Outpost24 Advisory, July 16, 2002.
1563 Debian Security Advisory, DSA-104-1, January 14, 2002.
1564 Red Hat Security Advisory, RHSA-2002:007-16, January 22, 2002.
1565 FreeBSD Security Advisory, FreeBSD-SA-01:68, December 17, 2001.
1566 Securiteam, August 28, 2002.
1567 Bugtraq, August 25, 2002.
1568 Bugtraq, July 1, 2002.
1569 Securiteam, May 4, 2002.
1570 SuSE Security Announcement, SuSE-SA:2002:047, December 6, 2002.
1571 Vapid Labs Advisory, October 11, 2002.
1572 Securiteam, November 24, 2002.
1573 Bugtraq, February 25, 2002.
1574 SecurityFocus, May 24, 2002.
1575 SecurityFocus, May 24, 2002.
1576 SecurityFocus, May 24, 2002.
1577 SecurityFocus, March 22, 2002.
1578 Bugtraq, March 31, 2002.
1579 Bugtraq, April 11, 2002.
1580 Bugtraq, May 9, 2002.
1581 Bugtraq, May 27, 2002.
1582 OpenBSD Security Advisory, August 11, 2002.
1583 SecurityFocus, October 2, 2002.
1584 SecurityTracker Alert ID, 1005553, November 7, 2002.
1585 Bugtraq, November 20, 2002.
1586 Red Hat Security Advisory, RHSA-2002:014-07, January 22, 2002.
1587 Bugtraq, April 21, 2002.
1588 CERT® Advisory CA-2002-24, August 1, 2002. .
1589 SuSE Security Announcement, SuSE-SA:2002:043, November 12, 2002.
1590 CERT® Advisory CA-2002-23, July 30, 2002.
1591 Debian Security Advisory, DSA-136-1, July 30, 2002.
1592 Trustix Secure Linux Security Advisory, TSLSA-2002-0063, July 30, 2002.
1593 OpenPKG Security Advisory, OpenPKG-SA-2002.008, July 30, 2002.
1594 Gentoo Linux Security Announcement, July 30, 2002.
1595 Mandrake Linux Security Update Advisory, MDKSA-2002:046 1, August 6, 2002.
1596 SuSE Security Announcement, SuSE-SA:2002:027, July 30, 2002.
1597 Conectiva Linux Security Announcement, CLA-2002:513, July 31, 2002.
1598 Caldera International, Inc. Security Advisory, CSSA-2002-033.1, August 2, 2002.
1599 EnGarde Secure Linux Security Advisory, ESA-20020730-019, July 30, 2002.
1600 CERT® Advisory, CA-2002-27, September 17, 2002.
1601 CERT® Advisory CA-2002-23, July 30, 2002.
1602 Debian Security Advisory, DSA-136-1, July 30, 2002.
1603 Trustix Secure Linux Security Advisory, TSLSA-2002-0063, July 30, 2002.
1604 OpenPKG Security Advisory, OpenPKG-SA-2002.008, July 30, 2002.
1605 Gentoo Linux Security Announcement, July 30, 2002.
1606 Mandrake Linux Security Update Advisory, MDKSA-2002:046 1, August 6, 2002.
1607 SuSE Security Announcement, SuSE-SA:2002:027, July 30, 2002.
1608 Conectiva Linux Security Announcement, CLA-2002:513, July 31, 2002.
1609 Caldera International, Inc. Security Advisory, CSSA-2002-033.1, August 2, 2002.
1610 EnGarde Secure Linux Security Advisory, ESA-20020730-019, July 30, 2002.
1611 EnGarde Secure Linux Security Advisory, ESA-20020807-020, August 7, 2002.
1612 RedHat Security Advisory, RHSA-2002:160-21, August 5, 2002.
1613 Conectiva Linux Security Announcement, CLA-2002:516, August 8, 2002.
1614 SecurityFocus, March 10, 2002.
1615 Geekgang Security Advisory, GSA2002-01, February 12, 2002.
1616 Sandblad Advisory #6, May 15, 2002.
1617 GreyMagic Security Advisory, GM#001-OP, May 27, 2002.
1618 Bugtraq, August 6, 2002.
1619 sp00fed packet advisory #2, September 15, 2002.
1620 SecurityFocus, November 21, 2002.

1621 SecurityTracker Alert ID, 1005634, November 14, 2002.
1622 NGSSoftware Insight Security Research Advisory, NISR20122001, December 21, 2001.
1623 Oracle Security Alert #27, December 28, 2001.
1624 SecurityFocus, January 18, 2002.
1625 SecurityFocus, January 17, 2002.
1626 SecurityFocus, January 17, 2002.
1627 SecurityFocus, January 18, 2002.
1628 NGSSoftware Insight Security Research Advisory, NISR06022002A, February 6, 2002.
1629 NGSSoftware Insight Security Research Advisory, NISR06022002C, February 6, 2002.
1630 NGSSoftware Insight Security Research Advisory, NISR06022002B, February 6, 2002.
1631 CERT Advisory, CA-2002-08, March 15, 2002.
1632 CERT Advisory, CA-2002-08, March 15, 2002.
1633 CERT Advisory, CA-2002-08, March 15, 2002.
1634 CERT Advisory, CA-2002-08, March 15, 2002.
1635 Oracle Security Alert #31, April 1, 2002.
1636 Bugtraq, April 1, 2002.
1637 Bugtraq, March 28, 2002.
1638 SecurityFocus, April 16, 2002.
1639 AngryPacket Security Advisory, 0x0004, July 17, 2002.
1640 Oracle Security Alert #41, August 14, 2002.
1641 NGSSoftware Insight Security Research Advisory, #NISR14082002, August 14, 2002.
1642 Internet Security Systems Security Bulletin, August 13, 2002.
1643 Oracle Security Alert #44, October 4, 2002.
1644 Rapid 7, Inc. Security Advisory, R7-0006, October 9, 2002.
1645 Oracle Security Alert #43, October 4, 2002.
1646 Oracle Security Alert #46, October 31, 2002.
1647 Bugtraq, August 15, 2002.
1648 Bugtraq, June 16, 2002.
1649 Securiteam, May 2, 2002.
1650 Securiteam, July 24, 2002.
1651 iDEFENSE Security Advisory, 11.04.02a, November 4, 2002.
1652 Westpoint Security Advisory, wp-02-0012, July 10, 2002.
1653 Mandrake Linux Security Update Advisory, MDKSA-2002:075, November 7, 2002.
1654 Bugtraq, January 23, 2002.
1655 Bugtraq, July 31, 2002.
1656 Securiteam, May 6, 2002.
1657 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:089-07, June 9, 2002.
1658 SecurityFocus, April 11, 2002.
1659 NTBugtraq, December 2, 2002.
1660 Bugtraq, November 8, 2002.
1661 Bugtraq, November 8, 2002.
1662 Securiteam, November 18, 2002.
1663 SecurityFocus, November 18, 2002.
1664 Bugtraq, October 24, 2002.
1665 SCAN Associates Advisory, October 18, 2002.
1666 SCAN Associates Advisory, October 18, 2002.
1667 SCAN Associates Advisory, October 18, 2002.
1668 iDEFENSE Security Advisory, 11.08.02a, November 8, 2002.
1669 INTEXXIA(c) Security Advisory, 1050-181201, December 18, 2001.
1670 Bugtraq, April 21, 2002.
1671 Securiteam, March 2, 2002.
1672 SecurityFocus, May 14, 2002.
1673 Bugtraq, May 18, 2002.
1674 Bugtraq, May 18, 2002.
1675 Security Advisory, DW020203-PHP, February 3, 2002.
1676 ALPER Research Labs Security Advisory, ARL02-A05, March 12, 2002.
1677 SecurityFocus, April 30, 2002.
1678 Securiteam, April 23, 2002.
1679 Bugtraq, July 23, 2002.
1680 e-matters GmbH Security Advisory, July 22, 2002.
1681 Securiteam, September 9, 2002.
1682 Bugtraq, October 20, 2002.
1683 Bugtraq, October 20, 2002.
1684 Bugtraq, July 2, 2002.
1685 Advisory #3, February 7, 2002.
1686 Bugtraq, August 23, 2002.
1687 SecurityFocus, November 29, 2002.
1688 Securiteam, January 15, 2002.
1689 Securiteam, September 11, 2002.

1690 Debian Security Advisory, DSA 168-1, September 18, 2002.
1691 SuSE Security Announcement, SuSE-SA:2002:036, October 7, 2002.
1692 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:213-06, November 11, 2002.
1693 Securiteam, June 18, 2002.
1694 ITCF Advisory 5, March 21, 2002.
1695 Whitecell Security Systems, WSS-Advisories-02003, April 4, 2002.
1696 Bugtraq, March 18, 2002.
1697 Bugtraq, May 26, 2002.
1698 Bugtraq, June 16, 2002.
1699 Bugtraq, October 9, 2002.
1700 Bugtraq, October 27, 2002.
1701 Bugtraq, November 18, 2002.
1702 Sec-Tec Advisory, November 25, 2002.
1703 Bugtraq, December 3, 2002.
1704 Bugtraq, October 10, 2002.
1705 Bugtraq, September 9, 2002.
1706 Bugtraq, September 9, 2002.
1707 Bugtraq, September 9, 2002.
1708 Bugtraq, April 3, 2002.
1709 Bugtraq, October 3, 2002.
1710 SecurityFocus, October 3, 2002.
1711 Bugtraq, March 18, 2002.
1712 Bugtraq, April 25, 2002.
1713 Securiteam, March 16, 2002.
1714 Bugtraq, October 10, 2002.
1715 ALPER Research Labs Security Advisory, ARL02-A12, June 6, 2002.
1716 Bugtraq, January 29, 2002.
1717 Securiteam, April 29, 2002.
1718 SecurityFocus, April 29, 2002.
1719 SecurityFocus, February 1, 2002.
1720 Bugtraq, July 16, 2002.
1721 Conectiva Linux Security Announcement, CLA-2002:549, November 18, 2002.
1722 @stake Inc. Security Advisory, A071202-1, July 12, 2002.
1723 Sys-Security Group Security Advisory, August 20, 2002.
1724 Bugtraq, June 21, 2002.
1725 Bugtraq, January 20, 2002.
1726 UkR Security Team Advisory, September 14, 2002.
1727 SecurityFocus, January 23, 2002.
1728 TWLC Security Advisory, December 21, 2001.
1729 SecurityFocus, January 7, 2002.
1730 KPMG-2002018, May 7, 2002.
1731 Internet Security Systems, September 4, 2002.
1732 Polycom Security Advisory 02-002, October 15, 2002.
1733 SecurityFocus, November 28, 2002.
1734 SecurityFocus, February 6, 2002.
1735 SecurityFocus, February 6, 2002.
1736 Securiteam, March 28, 2002.
1737 Bugtraq, April 20, 2002.
1738 Bugtraq, April 16, 2002.
1739 @(#) Mordred Labs Advisory, 0x0001, August 19, 2002.
1740 @(#) Mordred Labs Advisory 0x0003, August 20, 2002.
1741 @(#) Mordred Labs Advisory 0x0004, August 20, 2002.
1742 Bugtraq, March 28, 2002.
1743 Bugtraq, March 22, 2002.
1744 Bugtraq, September 25, 2002.
1745 Bugtraq, September 25, 2002.
1746 SecurityFocus, April 9, 2002.
1747 Bugtraq, October 2, 2002.
1748 Securiteam, February 18, 2002.
1749 Securiteam, March 2, 2002.
1750 Bugtraq, December 8, 2002.
1751 Bugtraq, April 1, 2002.
1752 Bugtraq, May 2, 2002.
1753 CERT Advisory, CA-2000-02, February 2, 2002.
1754 INetCop Security Advisory, 2002-0x82-005, November 24, 2002.
1755 Securiteam, December 1, 2002.
1756 Bugtraq, January 22, 2002.
1757 Bugtraq, April 22, 2002.
1758 SecurityFocus, April 17, 2002.

1759 Debian Security Advisory, DSA-166-1, September 13, 2002.
1760 Telhack Security Advisory - #1, April 18, 2002.
1761 SecurityTracker Alert ID, 1005726, November 28, 2002.
1762 Bugtraq, October 2, 2002.
1763 Securiteam, July 22, 2002.
1764 Bugtraq, July 17, 2002.
1765 Bugtraq, July 17, 2002.
1766 Debian Security Advisory, DSA 159-1, August 28, 2002.
1767 Bugtraq, June 3, 2002.
1768 Bugtraq, June 3, 2002.
1769 Securiteam, November 24, 2002.
1770 Securiteam, November 24, 2002.
1771 Bugtraq, May 31, 2002.
1772 Securiteam, November 7, 2002.
1773 iDEFENSE Security Advisory, 11.08.02b, November 8, 2002.
1774 SecurityFocus, March 18, 2002.
1775 Bugtraq, March 15, 2002.
1776 GreyMagic Security Advisory, GM#002-IE, March 22, 2002.
1777 Bugtraq, April 29, 2002.
1778 SNS Advisory No.55, August 8, 2002.
1779 Bugtraq, August 8, 2002.
1780 Bugtraq, November 13, 2002.
1781 Bugtraq, May 30, 2002.
1782 iDEFENSE Security Advisory, 10.15.02, October 15, 2002.
1783 Bugtraq, October 23, 2002.
1784 Guardeon Solutions AG Security Advisory, 03-2002, November 22, 2002.
1785 Bugtraq, September 3, 2002.
1786 Debian Security Advisory, DSA 164-1, September 10, 2002.
1787 Bugtraq, March 27, 2002.
1788 SecurityFocus, January 8, 2002.
1789 Bugtraq, March 2, 2002.
1790 NtWaK0 Advisory, February 27, 2002.
1791 Shadow Penguin Security Advisory #48, July 12, 2002.
1792 Shadow Penguin Security Advisory #47, July 12, 2002.
1793 NGSSoftware Insight Security Research Advisory, NISR22112002, November 22, 2002.
1794 SecurityFocus, December 11, 2002.
1795 Securiteam, May 6, 2002.
1796 SecurityFocus, March 4, 2002.
1797 RedHat Security Advisory, RHSA-2002:062-08, May 1, 2002.
1798 Bugtraq, May 21, 2002.
1799 Bugtraq, June 11, 2002.
1800 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:162-12, August 30, 2002.
1801 SCO Security Advisory, CSSA-2002-044.0, November 11, 2002.
1802 @stake Inc. Security Advisory, June 5, 2002.
1803 Bugtraq, November 1, 2002.
1804 secondmotion-SM-SA-02-03 Security Advisory, November 6, 2002.
1805 Securiteam, February 22, 2002.
1806 WhiteHat Security Advisory 1004, November 11, 2002.
1807 SecurityFocus, June 12, 2002.
1808 Bugtraq, February 26, 2002.
1809 sp00fed packet advisory #1, June 27, 2002.
1810 Bugtraq, May 12, 2002.
1811 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:107-11, August 5, 2002.
1812 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:098-14, August 5, 2002.
1813 Hewlett-Packard Company Security Advisory, HPSBTL0208-057, August 6, 2002.
1814 Mandrake Linux Security Update Advisory, MDKSA-2002:054, August 1, 2002.
1815 Mandrake Linux Security Update Advisory, MDKSA-2002:054, August 1, 2002.
1816 Gentoo Linux Security Announcement, August 27, 2002.
1817 Debian Security Advisory, DSA 158-1, August 27, 2002.
1818 Bugtraq, July 30, 2002
1819 Mandrake Linux Security Update Advisory, MDKSA-2002:024, March 13, 2002.
1820 Securiteam, September 12, 2002.
1821 Bugtraq, September 23, 2002.
1822 Bugtraq, June 13, 2002.
1823 Bugtraq, November 13, 2002.
1824 iDEFENSE Security Advisory 10.16.02, October 16, 2002.
1825 SecurityTracker Alert ID 1005544, November 6, 2002.
1826 Bugtraq, September 27, 2002.
1827 FreeBSD Security Notice, FreeBSD-SN-02:05, August 28, 2002.

1828 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:266-05, November 22, 2002.
1829 Conectiva Linux Security Announcement, CLA-2002:550, November 22, 2002.
1830 SuSE Security Announcement, SuSE-SA:2002:045, November 20, 2002.
1831 Gentoo Linux Security Announcement , 200211-007, November 21, 2002.
1832 Debian Security Advisory, DSA-200-1, November 22, 2002.
1833 Mandrake Linux Security Update Advisory, MDKSA-2002:081, November 26, 2002.
1834 Trustix Secure Linux Security Advisory, 2002-0080, November 25, 2002.
1835 VulnWatch, January 16, 2002.
1836 NGSSoftware Insight Security Research Advisory, NISR01042002, April 1, 2002.
1837 KPMG-2002012, April 18, 2002.
1838 Bugtraq, January 28, 2002.
1839 Bugtraq, April 27, 2002.
1840 SAP DB Security Alert, December 2, 2002.
1841 Securiteam, December 8, 2002.
1842 Shadow Penguin Security Advisory #42, January 10, 2002.
1843 SN-004201, January 29, 2002.
1844 Bugtraq, January 30, 2002.
1845 PivX Security Advisory, September 13, 2002.
1846 Foundstone Inc. Advisory, 091002-SVWS, September 10, 2002.
1847 Warped Force Advisory #2, February 11, 2002.
1848 Strategic Reconnaissance Team Security Advisory, SRT2002-06-11-1037, June 10, 2002.
1849 DownBlood Security Research Lab Advisory, June 12, 2002.
1850 Bugtraq, October 8, 2002.
1851 Securiteam, June 11, 2002.
1852 Phenoelit Advisory, July 27, 2002.
1853 Bugtraq, May 23, 2002.
1854 SecurityFocus, June 28, 2002.
1855 Bugtraq, September 21, 2002.
1856 iDEFENSE Security Advisory, 10.01.02, October 1, 2002.
1857 CERT® Advisory CA-2002-28, October 8, 2002.
1858 Gobbles Security Labs, June 13, 2002.
1859 SGI Security Advisory, 20020102-03-P, January 16, 2002.
1860 SGI Security Advisory, 20020103-01-I, January 28, 2002.
1861 SGI Security Advisory, 20020201-01-P, April 3, 2002.
1862 SGI Security Advisory, 20020306-01-P, March 28, 2002.
1863 SGI Security Advisory, 20020401-01-P, April 10, 2002.
1864 SGI Security Advisory, 20020402-01-P, April 15, 2002.
1865 SGI Security Advisory, 20020406-01-P, April 24, 2002.
1866 SGI Security Advisory, 20020409-01-I, April 30, 2002.
1867 SGI Security Advisory, 20020405-01-I, April 24, 2002.
1868 SGI Security Advisory, 20020407-01-I, April 30, 2002.
1869 SGI Security Advisory, 20020408-01-I, April 30, 2002.
1870 SGI Security Advisory, 20020501-01-I, May 1, 2002.
1871 SGI Security Advisory, 20020404-01-P, April 24, 2002.
1872 SGI Security Advisory, 20020504-01-I, May 8, 2002.
1873 SGI Security Advisory, 20020503-01-I, May 7, 2002.
1874 SGI Security Advisory, 20020602-01-I, June 6, 2002.
1875 SGI Security Advisory, 20020601-01-P, June 4, 2002.
1876 SGI Security Advisory, 20020605-01-I, June 20, 2002.
1877 SGI Security Advisory, 20020607-02-I, June 24, 2002.
1878 SGI Security Advisory, 20020805-01-I, August 14, 2002.
1879 SGI Security Advisory, 20020804-01-P, August 12, 2002.
1880 SGI Security Advisory, 20020305-03-I, August 14, 2002.
1881 SGI Security Advisory, 20020902-01-I, September 18, 2002.
1882 SGI Security Advisory, 20020903-01-P, October 14, 2002.
1883 Bugtraq, March 5, 2002.
1884 Bugtraq, September 25, 2002.
1885 Bugtraq, July 25, 2002.
1886 Syracuse University Security Advisory, SURUAZ-2002-07-07, July 10, 2002.
1887 Xfocus, January 14, 2002.
1888 Securiteam, July 1, 2002.
1889 Bugtraq, February 16, 2002.
1890 Global InterSec LLC Advisory, 2002021001, October 16, 2002.
1891 SA-2002:00, January 10, 2002.
1892 SA-2002:01, February 19, 2002.
1893 Bugtraq, April 22, 2002.
1894 Security Advisory #4, July 23, 2002.
1895 Debian Security Advisory, DSA 203-1, December 4, 2002.
1896 KPMG-2002017, May 2, 2002.

1897 Securiteam, January 22, 2002.
1898 Bugtraq, February 27, 2002.
1899 Bugtraq, April 19, 2002.
1900 Securiteam, November 6, 2002
1901 InterSec Security Advisory, October 18, 2002.
1902 Bugtraq, October 24, 2002.
1903 iDEFENSE Security Advisory, 10.24.02, October 24, 2002.
1904 Securiteam, May 18, 2002.
1905 Bugtraq, October 29, 2002.
1906 Sony Security Announcement, January 25, 2002.
1907 Bugtraq, November 5, 2002.
1908 Securiteam, March 26, 2002.
1909 Bugtraq, June 6, 2002.
1910 SecurityFocus, January 3, 2002.
1911 Bugtraq, January 24, 2002.
1912 Bugtraq, January 24, 2002.
1913 Bugtraq, March 28, 2002.
1914 SecurityFocus, May 3, 2002.
1915 Bugtraq, December 3, 2002.
1916 Bugtraq, September 19, 2002.
1917 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:204-10, October 9, 2002.
1918 Debian Security Advisory, DSA 191-2, November 11, 2002.
1919 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:204-10, October 9, 2002.
1920 Debian Security Advisory, DSA 191-2, November 11, 2002.
1921 Bugtraq, April 18, 2002.
1922 Bugtraq, May 23, 2002.
1923 SSH Communications Advisory, November 25, 2002.
1924 SSH Communications Security Advisory, November 25, 2002.
1925 Bugtraq, February 21, 2002.
1926 David Evlis Reign Security Advisory #11, June 4, 2002.
1927 Bugtraq, August 21, 2002.
1928 Strategic Reconnaissance Team Security Advisory, SRT2002-06-04-1011, June 4, 2002.
1929 Securiteam, April 14, 2002.
1930 Superpetz Advisory #001, January 28, 2002.
1931 EnGarde Secure Linux Security Advisory, ESA-20011227-01, December 27, 2001.
1932 Red Hat Security Advisory, RHSA-2002:002-10, January 3, 2002.
1933 Bugtraq, August 19, 2002.
1934 Securiteam, February 25, 2002.
1935 Securiteam, April 22, 2002.
1936 Securiteam, June 28, 2002.
1937 Securiteam, July 18, 2002.
1938 Securiteam, December 28, 2001.
1939 SecurityFocus, January 30, 2002.
1940 SecurityFocus, February 14, 2002.
1941 Securiteam, March 2, 2002.
1942 Sun Microsystems, Inc. Security Bulletin, SUN-00216, March 5, 2002.
1943 Bugtraq, March 8, 2002.
1944 Bugtraq, March 11, 2002.
1945 NSFOCUS Security Advisory, SA2002-01, April 2, 2002.
1946 eSecurityOnline Security Advisory 4197, April 29, 2002
1947 eSecurityOnline Security Advisory 4123, April 29, 2002.
1948 eSecurityOnline Security Advisory 3761, April 29, 2002
1949 eSecurityOnline Security Advisory 4198, April 29, 2002.
1950 eSecurityOnline Security Advisory 2397, April 29, 2002.
1951 CERT Advisory, CA-2002-10, May 1, 2002.
1952 CERT Advisory CA-2002-11, May 6, 2002.
1953 SecurityFocus, May 13, 2002.
1954 eSecurityOnline Advisory 5063, May 20, 2002.
1955 DER Adv #7, May 22, 2002.
1956 Next Generation Security Technologies Security Advisory, NGSEC-2002-3, May 23, 2002.
1957 Sun Microsystems, Inc. Security Bulletin, #00219, June 4, 2002.
1958 Bugtraq, June 17, 2002.
1959 SecurityFocus, June 22, 2002.
1960 SecurityFocus, July 4, 2002.
1961 Sun(sm) Alert Notification, 45693, July 10, 2002.
1962 Bugtraq, July 7, 2002.
1963 SecurityFocus, July 5, 2002.
1964 Trust Factory Security Advisory, TF20020601, July 3, 2002.
1965 Portcullis Security Advisory, July 11, 2002.

1966 Bugtraq, July 17, 2002.
1967 Sun(sm) Alert Notification, 27807, July 22, 2002.
1968 Sun(sm) Alert Notification, 45707, July 10, 2002.
1969 Sun(sm) Alert Notification, 43908, July 22, 2002.
1970 Bugtraq, August 1, 2002.
1971 SecurityFocus, August 2, 2002.
1972 SecurityFocus, August 21, 2002.
1973 Sun Alert, 113176, August 21, 2002.
1974 SecurityFocus, August 15, 2002.
1975 Sun Microsystems Alert, 110286-09, August 29, 2002.
1976 Sun(sm) Alert Notification, 46988, September 10, 2002.
1977 SecurityFocus, November 25, 2002.
1978 Sun(sm) Alert Notification, 46903, September 11, 2002.
1979 Bugtraq, October 2, 2002.
1980 Sun(sm) Alert Notification, 47815, October 17, 2002.
1981 Sun(sm) Alert Notification, 48067, October 31, 2002.
1982 Sun(sm) Alert Notification, 48320, October 29, 2002.
1983 Sun(sm) Alert Notification, 48601, November 8, 2002.
1984 Next Generation Security Technologies Security Advisory, November 19, 2002.
1985 Bugtraq, November 27, 2002.
1986 CERT/CC VU#810921 Note, December 11, 2002.
1987 Sun(sm) Alert Notification, 46867, December 4, 2002.
1988 Sun(sm) Alert Notification, 48267, December 2, 2002.
1989 Sun(sm) Alert Notification, 48216, November 27, 2002.
1990 Bugtraq, September 29, 2002.
1991 eEye Digital Security Advisory, August 8, 2002.
1992 SecurityTracker Alert IDs, 1005701 & 1005702, November 26, 2002.
1993 Sun(sm) Alert Notification, 49304, December 9, 2002.
1994 Arhont Ltd. Information Security Advisory, November 13, 2002.
1995 Westpoint Security Advisory, wp--02-0005, October 2, 2002.
1996 Bugtraq, October 9, 2002.
1997 Vuln-Dev, March 9, 2002.
1998 SuSE Security Announcement: shadow, SuSE-SA:2002:017, May 16, 2002.
1999 SuSE Security Announcement, SuSE-SA:2002:016, May 8, 2002.
2000 SuSE Security Announcement, SuSE-SA:2002:032, September 18, 2002.
2001 SuSE Security Announcement, SuSE-SA:2002:040, October 31, 2002.
2002 Debian Security Advisory, DSA 192-1, November 8, 2002.
2003 SecurityFocus, November 25, 2002.
2004 Debian Security Advisory, DSA 192-2, December 6, 2002.
2005 Bugtraq, September 3, 2002.
2006 Bugtraq, September 3, 2002.
2007 SHATTER Team Security Alert, November 26, 2002.
2008 SHATTER Team Security Alert, November 26, 2002.
2009 SHATTER Team Security Alert, November 26, 2002.
2010 Bugtraq, February 9, 2002.
2011 Corsaire Limited Security Advisory, February 20, 2002.
2012 Bugtraq, February 26, 2002.
2013 Bugtraq, February 25, 2002.
2014 Edvice Security Services, March 7, 2002.
2015 Bugtraq, April 15, 2002.
2016 Bugtraq, April 16, 2002.
2017 Bugtraq, April 16, 2002.
2018 @stake, Inc. Security Advisory, A071502-1, July 15, 2002.
2019 Ubizen Security Advisory, August 2, 2002.
2020 Securiteam, September 12, 2002.
2021 Advanced IT-Security Advisory #01-10-2002, October 14, 2002.
2022 Advanced IT-Security Advisory #02-10-2002, October 14, 2002.
2023 Symantec Security Advisory, October 15, 2002.
2024 SecurityFocus, October 7, 2002.
2025 Bugtraq, November 20, 2002.
2026 Bugtraq, March 30, 2002.
2027 Bugtraq, July 30, 2002.
2028 SECURITY.NNOV Notification, July 26, 2002.
2029 NGSSoftware Insight Security Research Advisory, NISR01032002A, March 5, 2002.
2030 NGSSoftware Insight Security Research Advisory, NISR13032002, March 13, 2002.
2031 NGSSoftware Insight Security Research Advisory, NISR17042002B, April 17, 2002.
2032 Bugtraq, January 26, 2002.
2033 Bugtraq, February 19, 2000.
2034 SecurityFocus, April 9, 2002.

2035 SecurityFocus, June 3, 2002.
2036 SecurityFocus, June 3, 2002.
2037 Securiteam, October 15, 2002.
2038 Bugtraq, June 5, 2002.
2039 Bugtraq, November 18, 2002.
2040 Bugtraq, November 18, 2002.
2041 SecurityFocus, February 25, 2002.
2042 SecurityTracker Alert ID 1005587, November 8, 2002.
2043 Bugtraq, February 22, 2002.
2044 SecurityFocus, May 11, 2002.
2045 Security Bugware, June 5, 2002.
2046 SecurityFocus, July 16, 2002.
2047 SecurityFocus, July 16, 2002.
2048 SecurityFocus, February 6, 2002.
2049 Bugtraq, October 2, 2002.
2050 Bugtraq, July 24, 2002.
2051 Securiteam, December 21, 2001.
2052 Bugtraq, January 9, 2002.
2053 Bugtraq, February 28, 2002.
2054 NSSI-Research Labs Security Advisory, NSSI-2002-tpfw, August 20, 2002.
2055 Debian Security Advisory, DSA 172-1, October 8, 2002.
2056 SuSE Security Announcement, SuSE-SA:2002:002, January 14, 2002.
2057 EnGarde Secure Linux Security Advisory, ESA-20020114-001, January 14, 2002.
2058 Debian Security Advisory, DSA 101-1, January 14, 2002.
2059 RedHat Security Advisory, RHSA-2002:011-06, January 15, 2002.
2060 FreeBSD Security Advisory, FreeBSD-SA-02:06, January 16, 2002.
2061 Immunix OS Security Advisory, IMNX-2002-70-001-01, January 17, 2002.
2062 Trustix Secure Linux Security Advisory #2002-0021, January 18, 2002.
2063 Bugtraq, January 26, 2002.
2064 Bugtraq, September 13, 2002.
2065 NGSSoftware Insight Security Research Advisory, #NISR19082002B, August 19, 2002.
2066 Bugtraq, December 28, 2001.
2067 Securiteam, May 28, 2002.
2068 SNS Advisory No.54, June 13, 2002.
2069 Inside Security GmbH Vulnerability Notification, March 10, 2002.
2070 Bugtraq, April 24, 2002.
2071 Bugtraq, May 24, 2002.
2072 Securiteam, July 17 2002.
2073 Securiteam, September 12, 2002.
2074 Bugtraq, December 5, 2002.
2075 Texonet Security Advisory 20021210, December 10, 2002.
2076 PivX Security Advisory, August 28, 2002.
2077 Bugtraq, September 29, 2002.
2078 Bugtraq, April 15, 2002.
2079 Securiteam, November 28, 2002.
2080 Bugtraq, August 25, 2002.
2081 SecurityFocus, September 6, 2002.
2082 Bugtraq, October 2, 2002.
2083 Bugtraq, December 7, 2002.
2084 Securiteam, July 12, 2002.
2085 Bugtraq, March 23, 2002.
2086 Bugtraq, July 25, 2002.
2087 Bugtraq, October 2, 2002.
2088 SecurityFocus, February 21, 2002.
2089 Bugtraq, December 4, 2002.
2090 Debian Security Advisory, DSA 097-1, January 3, 2002.
2091 Red Hat Security Advisory, RHSA-2001:176-05, January 7, 2002.
2092 Bugtraq, August 19, 2002.
2093 FreeBSD Security Advisory, FreeBSD-SA-02:05, January 10, 2002.
2094 Bugtraq, June 7, 2002.
2095 Bugtraq, July 24, 2002.
2096 Bugtraq, November 7, 2002.
2097 Securiteam, February 15, 2002.
2098 SNS Advisory No.53, May 7, 2002.
2099 SNS Advisory No.52, May 7, 2002.
2100 Bugtraq, August 23, 2002.
2101 Bugtraq, June 20, 2002.
2102 VanDyke Technologies Security Advisory, July 25, 2002.
2103 SecurityFocus, March 21, 2002.

2104 Bugtraq, March 20, 2002.
2105 Bugtraq, December 8, 2002.
2106 Bugtraq, October 9, 2002.
2107 Bugtraq, October 8, 2002.
2108 Securiteam, March 26, 2002.
2109 SecurityTracker, September 9, 2002.
2110 Point Blank Security, June 26, 2002.
2111 Securiteam, May 19, 2002.
2112 SecurityFocus, April 29, 2002.
2113 Kowchews Security Advisory, May 27, 2002.
2114 Bugtraq, October 31, 2002.
2115 Bugtraq, October 31, 2002.
2116 Bugtraq, July 25, 2002.
2117 Bugtraq, July 24, 2002.
2118 Bugtraq, June 6, 2002.
2119 Centaura Technologies Security Research Lab Advisory, October 24, 2002.
2120 Securiteam, April 22, 2002.
2121 Securiteam, January 11, 2002.
2122 KPMG-2002031, July 17, 2002.
2123 KPMG-2002034, July 17, 2002.
2124 Bugtraq, August 11, 2002.
2125 Bugtraq, August 17, 2002.
2126 Bugtraq, January 23, 2002.
2127 Securiteam, October 1, 2002.
2128 Caldera International, Inc. Security Advisory, CSSA-2002-021.0, May 15, 2002.
2129 Bugtraq, June 1, 2002.
2130 KPMG-2002008, April 10, 2002.
2131 Securiteam, September 30, 2002.
2132 KPMG-2002007, April 8, 2002.
2133 KPMG-2002030, July 9, 2002.
2134 KPMG-2002027, July 1, 2002.
2135 SecurityFocus, November 25, 2002.
2136 Securiteam, August 21, 2002.
2137 Bugtraq, December 17, 2001.
2138 Securiteam, March 22, 2002.
2139 Securiteam, March 22, 2002.
2140 Bugtraq, March 20, 2002.
2141 Securiteam, August 27, 2002.
2142 FreeBSD Security Advisory, FreeBSD-SN-02:06, October 10, 2002.
2143 Nerf gr0up: adv #7, June 18, 2002.
2144 Bugtraq, August 15, 2002.
2145 Bugtraq, March 25, 2002.
2146 Securiteam, December 2, 2002.
2147 NGSSoftware Insight Security Research Advisory, NISR17042002C, April 17, 2002.
2148 Debian Security Advisory, DSA 139-1, August 1, 2002.
2149 Debian Security Advisory, DSA-190-1, November 7, 2002.
2150 Debian Security Advisory, DSA 108-1, February 7, 2002.
2151 iDEFENSE Security Advisory, 09.30.2002, September 30, 2002.
2152 Andrew Badr Security Advisory, June 17, 2002.
2153 Bugtraq, May 26, 2002.
2154 Bugtraq, April 13, 2002.
2155 Bugtraq, September 8, 2002.
2156 Guardent Client Advisory, September 6, 2002.
2157 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:188-08, September 9, 2002.
2158 Bugtraq, March 22, 2002.
2159 Bugtraq, April 19, 2002.
2160 Strumpf Noir Society Summaries, January 21, 2002.
2161 Strumpf Noir Society Advisories, February 26, 2002.
2162 Strumpf Noir Society Advisories, February 26, 2002.
2163 Bugtraq, June 1, 2002.
2164 SecurityFocus, June 23, 2002.
2165 Securiteam, July 9, 2002.
2166 SecurITeam News, July 8, 2002.
2167 Bugtraq, July 19, 2002.
2168 Bugtraq, July 13, 2002.
2169 Bugtraq, July 20, 2002.
2170 Securiteam, October 25, 2002.
2171 Bugtraq, November 24, 2002.
2172 Securiteam, November 24, 2002.

2173 Bugtraq, July 4, 2002.
2174 INetCop Security Advisory, 2002-0x82-006, November 25, 2002.
2175 Bugtraq, March 28, 2002.
2176 Bugtraq, September 12, 2002.
2177 Securiteam, January 11, 2002.
2178 Bugtraq, March 27, 2002.
2179 SecurityFocus, April 25, 2002.
2180 SecurityFocus, April 25, 2002.
2181 ITCP Advisory 12, April 14, 2002.
2182 Bugtraq, May 17, 2002.
2183 Bugtraq, October 3, 2002.
2184 Securiteam, March 8, 2002.
2185 Bugtraq, June 10, 2002.
2186 Bugtraq, October 3, 2002.
2187 Red Hat, Inc. Red Hat Bug Fix Advisory, RHBA-2002:080-09, May 9, 2002.
2188 Conectiva Linux Update Announcement, CLA-2002:486, May 13, 2002.
2189 Bugtraq, January 28, 2002.
2190 Debian Security Advisory, DSA 151-1, August 13, 2002.
2191 Gentoo Linux Security Announcement, August 14, 2002.
2192 Bugtraq, January 29, 2002.
2193 Bugtraq, January 29, 2002.
2194 Bugtraq, September 24, 2002.
2195 Securiteam, November 14, 2002.
2196 SecurityTracker Alert ID, 1005770, December 6, 2002.
2197 SecurityFocus, March 13, 2002.
2198 SecurityFocus, March 13, 2002.
2199 Securiteam, March 4, 2002.
2200 VulnWatch, January 9, 2002.
2201 EyeonSecurity, June 5, 2002.
2202 AngryPacket Security Advisory, 0x0003, June 21, 2002.
2203 Bugtraq, October 18, 2002.
2204 SecurityFocus, November 28, 2002.
2205 Bugtraq, February 21, 2002.
2206 Bugtraq, May 27, 2002.
2207 Bugtraq, November 6, 2002.
2208 Shadow Penguin Security #45, January 11, 2002.
2209 Qitest1 Security Advisory #004, July 12, 2002.
2210 PYR/MID, Research Project Security Advisory, October 14, 2002.
2211 Bugtraq, May 21, 2002.
2212 ECHU Alert #3, October 14, 2002.
2213 DownBload Security Research Lab Advisory, June 28, 2002.
2214 ALPER Research Labs Security Advisory, ARL02-A14, June 10, 2002.
2215 Bugtraq, February 21, 2002.
2216 JCC Security Advisory, June 15, 2002.
2217 Bugtraq, November 8, 2002.
2218 SecurityFocus, November 26, 2002.
2219 FreeBSD Security Notice, FreeBSD-SN-02:05, August 28, 2002.
2220 SecurityFocus, July 10, 2002.
2221 Bugtraq, April 2, 2002.
2222 Bugtraq, March 1, 2002.
2223 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:060-17, September 24, 2002.
2224 Bugtraq, October 1, 2002.
2225 Bugtraq, October 7, 2002.
2226 Zope Alert 2002-06-14, September 26, 2002.
2227 Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:060-17, September 24, 2002.
2228 Securiteam, December 19, 2001
2229 Bugtraq, March 11, 2002.
2230 Bugtraq, June 17, 2002.
2231 Bugtraq, July 24, 2002.