



National Infrastructure Protection Center CyberNotes: 2000 Year End Summary

Issue #2000-26

December 31, 2000

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. This special issue contains a summary of items covered in this publication during the past year.

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 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a year-end summary of software vulnerabilities identified between December 18, 1999 and December 14, 2000. 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.

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
@Stake Inc. ¹	AntiSniff 1.0.1; Researchers 1.0	Windows, Unix	AntiSniff DNS Overflow	High	CyberNotes 2000-10
3Rsoft ²	MailStudio-2000 2.9 & lower	Unix	3Rsoft Mailstudio Root Compromise	High	CyberNotes 2000-12
Acme ³	Thttpd 2.16-2.19	Unix	Thttpd Arbitrary World-Readable File Disclosure	Medium	CyberNotes 2000-20
Adcycle.com ⁴	Adcycle 0.77b		Adcycle Password Disclosure	Medium	CyberNotes-2000-24
Adobe ⁵	Acrobat Reader 3.0, 4.0, 4.05; Acrobat Business Tools 4.0, 4.05; Acrobat 3.0, 4.0, 4.05	Windows 95/98/NT 4.0/2000	Adobe Acrobat Reader Business Tools Buffer Overflow	High	CyberNotes 2000-15
AdTran Inc. ⁶	MX2800 M13		AdTran Ping Flood Denial of Service	Low	CyberNotes 2000-08
Akopia, Inc. ⁷	MiniVend 3.0, 4.0, 4.0.4		MiniVend Piped Command Execution	High	CyberNotes 2000-14
Alabanza Corporation ⁸	Alabanza Control Panel 3.0 and previous		Alabanza Control Panel Domain Modification	Medium	CyberNotes 2000-20
Aladdin Enterprises ⁹	Ghostsript 4.3, 5.10c1, 5.10.10, 5.10.15, 5.50	Unix	Ghostsript Arbitrary Shared Library Usage and Symlink	Medium	CyberNotes-2000-24
Aladdin Knowledge Systems ¹⁰	eToken 3.3.3x		Aladdin Knowledge Systems eToken PIN Extraction	Medium	CyberNotes 2000-09

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Alex Heiphetz Group, Inc. ¹¹	EZShopper 2.0, 3.0	Windows NT 4.0, Unix	EZShopper Directory Disclosure	Medium	CyberNotes-2000-25
Alex Heiphetz Group, Inc. ¹²	EZShopper 3.0	Windows NT 4.0, Unix	EZShopper Remote Command Execution	High	CyberNotes 2000-05
Alexander Siegel ¹³	Golddig 2.0	Unix	Golddig Game Arbitrary File Overwrite	High	CyberNotes 2000-10
Allaire ¹⁴	ClusterCATS ColdFusion		ClusterCATS URL Redirect	Medium	CyberNotes 2000-10
Allaire ¹⁵	Cold Fusion Server 4.5.x, Professional & Enterprise		ColdFusion Cached File Request Remote Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-10
Allaire ¹⁶	ColdFusion 4.5.1 and below	Windows NT/2000, Unix	Allaire ColdFusion Web Administrator Denial of Service	Low	CyberNotes 2000-12
Allaire ¹⁷	ColdFusion Server 4.0, 4.0.1, 4.5		Allaire ColdFusion Path Disclosure	Low	CyberNotes 2000-05
Allaire ¹⁸	ColdFusion Server 4.0x (all editions)		ColdFusion Information Exposure Vulnerability	Medium/Low	CyberNotes 2000-01
Allaire ¹⁹	ColdFusion Server 4.5.1		ColdFusion Sample Script Denial of Service	Low	CyberNotes-2000-25
Allaire ²⁰	Forums 2.x	Windows NT 4.0	Allaire Forums "RightAccessAllForums" Vulnerability	High	CyberNotes 2000-07
Allaire ²¹	JRun 2.3.x	Windows 95/98/NT 4.0/2000, Unix	JRun File Source Code Disclosure	Medium	CyberNotes-2000-22
Allaire ²²	JRun 2.3.x	Windows 95/98/NT 4.0/2000, Unix	JRun Arbitrary Code Execution	High	CyberNotes-2000-22
Allaire ²³	JRun 3.0	Windows 95/98/NT 4.0/2000, Unix	JRun Directory Disclosure	Medium	CyberNotes-2000-22
Allaire ²⁴	Spectra 1.0	Windows NT 4.0, Unix	Denial of Service Vulnerability	Low	CyberNotes 2000-01
Allaire ²⁵	Spectra 1.0	Windows NT 4.0, Unix	Spectra Unauthenticated RAS Access	Low	CyberNotes 2000-03
Allaire ²⁶	Spectra 1.0 Webtop	Windows NT 4.0, Unix	Privilege Elevation Vulnerability	Medium	CyberNotes 2000-01
Allaire ²⁷	Spectra 1.01	Windows NT, Unix	Spectra Administrative Interface	Medium	CyberNotes 2000-18
Allegro Software ²⁸	Rompager 2.10		Rompager Denial of Service	Low	CyberNotes 2000-12
AltaVista ²⁹	AltaVista Search Intranet v2.3a for NT, Tru64 and Solaris		Access Configuration File Vulnerability	High	CyberNotes 2000-01
Alt-N Technologies, Inc. ³⁰	MDaemon 2.8	Windows 95/98/NT 4.0/2000	MDaemon Session ID Hijacking	Medium	CyberNotes 2000-16
Alt-N Technologies, Inc. ³¹	MDaemon 3.5.1	Windows 95/98/NT 4.0/2000	MDaemon 'Lock Server' Bypass	High	CyberNotes-2000-25
Alt-N Technologies, Inc. ³²	WorldClient Standard 2.1	Windows NT	WorldClient Directory Traversal	Medium	CyberNotes 2000-14

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Alt-N Technologies, Inc. ³³	MDaemon 3.1.1	Windows 95/98/NT 4.0/2000	MDaemon Denial of Service	Low	CyberNotes 2000-19
AMaViS ³⁴	AMaViS 0.2-pre6-20000604	Unix	AMaViS TNEF Compression Support File Overwrite Vulnerability	High	CyberNotes 2000-14
America Online ³⁵	AOL Instant Messenger (AIM) version 4.1.2010	Windows 95/98/NT 4.0/2000	AOL Instant Messenger Denial of Service	Low	CyberNotes 2000-20
America Online ³⁶	Instant Messenger (AIM) 4.0	Windows 95/98/NT 4.0, CE 3.0; MacOS 9.0	AIM Path Disclosure	Medium	CyberNotes 2000-10
America Online ³⁷	Instant Messenger 3.5	Windows 95/98/NT 4.0/2000	AIM Denial of Service	Low	CyberNotes 2000-05
America Online ³⁸	AOL Instant Messenger (AIM)		AOL ICQ Buffer Overflow	High	CyberNotes 2000-02
AnalogX ³⁹	AnalogX SimpleServer:WWW HTTP Server v1.1		Buffer Overflow Vulnerability	High	CyberNotes 2000-01
AnalogX ⁴⁰	Proxy 4.04	Windows	Proxy Denial of Service	Low	CyberNotes 2000-15
AnalogX ⁴¹	Simple-Server WWW 1.05	Windows NT/2000	AnalogX SimpleServer Denial of Service	Low	CyberNotes 2000-12
AnalogX ⁴²	SimpleServer:WWW 1.0.6	Windows 95/98/NT 4.0	SimpleServer WWW Directory Traversal	Medium	CyberNotes 2000-15
AnalogX ⁴³	SimpleServerWWW 1.0.3, 1.0.4	Windows 95/98/NT 4.0	SimpleServer WWW Denial of Service	Low	CyberNotes 2000-07
Apache ⁴⁴	Apache versions 1.3.12 and prior		Apache Rewrite Arbitrary File Disclosure	Medium/High (High if network security best-practices not in place)	CyberNotes 2000-20, CyberNotes-2000-21
Apache Free Software Foundation ⁴⁵	Apache 1.3.6.12, 1.3.3, 1.3.6.2	Windows	Apache Root Directory Revealing	Medium	CyberNotes 2000-12
Apache Group ⁴⁶	Apache 1.3	Windows NT 4.0/2000	Apache Web Server with Php File Disclosure	Medium	CyberNotes-2000-25
Apple ⁴⁷	AppleShare IP 6.1-6.3	MacOS 9.0	AppleShare IP 6.x Invalid Range Request	Medium	CyberNotes 2000-09
Apple ⁴⁸	Macintosh OS9	MacOS	Denial of Service Vulnerability	Low	CyberNotes 2000-01
Ascend ⁴⁹	CascadeView B-STDx 8000/9000		Symbolic Link Vulnerability	High	CyberNotes 2000-01
Ashley Montanaro ⁵⁰	Darxite 0.4	Unix	Darxite Login Buffer Overflow	High	CyberNotes 2000-17
AT&T ⁵¹	WinVNC 3.3x	Windows 95/98/ME/NT 3.5/4.0/2000	WinVNC Remote Desktop Default Configuration	High	CyberNotes-2000-24
Atrium Software ⁵²	Cassandra NNTP Server 1.10	Windows 95/98/NT 4.0	Cassandra Buffer Overflow	Low	CyberNotes 2000-09
Atrium Software ⁵³	Mercur Mailserver 3.2 and below	Windows 95/98/NT	Mercur Mailserver Directory Traversal	Medium	CyberNotes 2000-09
Atrium Software ^{54, 55}	MERCUR Mailserver 3.2; POP3-Server v3.20.01; IMAP4-Server v3.20.01; WebMail-Client 1.0	Windows 95/98/NT 4.0	MERCUR Multiple Denial of Service Vulnerabilities	Low	CyberNotes 2000-06
A-V Tronics ⁵⁶	InetServ 3.0		A-V Tronics HTTP Get Request Buffer Overflow	High	CyberNotes 2000-02
aVirt ⁵⁷	Rover POP3 Server v1.1		POP3 Buffer Overflow Vulnerability	Low	CyberNotes 2000-01
aVirt ⁵⁸	aVirt Mail 4.0, 4.2	Windows 95/98/NT 4.0/2000	aVirt Mail 'Mail From:' and 'Rept to:' Denial of Service	Low	CyberNotes-2000-22

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
AVM ⁵⁹	KEN! 1.4.30, 1.3.10, 1.4.32	Windows 95/98 NT 4.0	AVM KEN! 1.3.10 Directory Traversal	Medium	CyberNotes 2000-08
AVT ⁶⁰	Rightfax Web Client v5.2	Windows NT 4.0	Rightfax Webclient Predictable Session Number	Medium	CyberNotes 2000-03
Axent ⁶¹	NetProwler 3.0	Windows NT 4.0	NetProwler Fragmented IP Packets Denial of Service	High	CyberNotes 2000-10
Axis Communications ⁶²	Axis 700 Network Scan Server 1.12		Axis 700 Authentication Bypass	Medium	CyberNotes 2000-03
Axis Communications ⁶³	StorPoint CD		Axis StorPoint CD Authentication	Medium	CyberNotes 2000-05
Bajie ⁶⁴	Java HTTP Server 1.0		Bajie Webserver Multiple Vulnerabilities	Medium	CyberNotes 2000-16
Balabit ⁶⁵	syslog-ng 1.4.8 and prior		Syslog-ng Incomplete Priority String Remote Denial of Service	Low	CyberNotes-2000-24
Bardon Data Systems ^{66, 67}	WinU 5.1 and previous	Windows 95/98/NT 4.0/2000	WinU Backdoor Password	High	CyberNotes-2000-21, CyberNotes-2000-22
BB4 Technologies ⁶⁸	Big Brother 1.4H and previous	MacOS, Unix	Big Brother Directory Traversal	Medium	CyberNotes 2000-14
BB4 Technologies ⁶⁹	Big Brother Network Monitor 1.5c2		Big Brother Arbitrary Shell Command Execution	High	CyberNotes-2000-21
Be Incorporated ⁷⁰	BeOS 5.0, 4.5	Windows 95/98/2000 NT4	BeOS 4.5/5.0 Invalid System Call	Low	CyberNotes 2000-08
BEA Systems ⁷¹	WebLogic Enterprise 5.1; WebLogic Express 5.1x; WebLogic Server 5.1x	Windows 98/NT 4.0/2000, Unix	WebLogic FileServlet Show Code	Medium	CyberNotes 2000-16
BEA Systems ⁷²	WebLogic Enterprise 5.1; WebLogic Express 5.1x; WebLogic Server 5.1x	Windows NT 4.0	WebLogic SSIServlet Show Code	High	CyberNotes 2000-16
BEA Systems ⁷³	WebLogic Express & Server 3.1.8, 4.0x, 4.5x, 5.1x	Windows 98/NT 4.0/2000, Unix	WebLogic Source Code Disclosure	Medium	CyberNotes 2000-13
BEA Systems ⁷⁴	Weblogic Server 3.1.8, 4.0x, 4.5x, 5.1x	Windows 98/NT 4.0/2000, Unix	Weblogic Proxy Multiple Buffer Overflow	High	CyberNotes 2000-17
Bill Kendrick ⁷⁵	GBook.cgi 1.0		Gbook.cgi Remote Command Execution	High	CyberNotes-2000-23
BinTec Communications ⁷⁶	ISDN router BIANCA/BRICK-XL; BIANCA/BRICK-XS		BinTec Router Security and Privacy Weakness	Medium	CyberNotes 2000-07
BisonWare ^{77, 78}	BisonWare FTP Server 3.5		Denial of Service Vulnerability	Low	CyberNotes 2000-05
Blackboard, Inc. ⁷⁹	CourseInfo 4.0	Windows NT 4.0	CourseInfo Plaintext Administrator Password	Medium	CyberNotes 2000-14
Blackboard, Inc. ⁸⁰	CourseInfo for Unix, CourseInfo 4.0	Windows NT 4.0, Unix	CourseInfo Database Modification	Medium	CyberNotes 2000-15
Borland/Inprise ⁸¹	InterBase SuperServer 6.0	Unix	Interbase SuperServer Denial of Service	Low	CyberNotes 2000-19
Bray Systems ⁸²	Linux Trustees 1.5 and prior	Unix	Bray Systems Trustees Long Pathname Denial of Service	Low	CyberNotes 2000-08
Brecht Claerhout ⁸³	Sniffit 0.3.7beta; Sniffit 0.3.6HIP	Unix	Sniffit Remote Buffer Overflow	High	CyberNotes 2000-09.
BroadGun Software ⁸⁴	CamShot WebCam 2.6 Trial Version	Windows 95/98/NT 4.0/2000	CamShot Remote Buffer Overflow	Medium	CyberNotes 2000-19
BroadGun Software ⁸⁵	CamShot WebCam v2.5	Windows 95/98/NT 4.0/2000	Buffer Overflow Vulnerability	High	CyberNotes 2000-01
BroadVision ⁸⁶	One-To-One Enterprise 1.0		One-To-One Enterprise Path Disclosure	Medium	CyberNotes-2000-25
BSDi ⁸⁷	BSD/OS 3.0, 3.1, 4.0, 4.0.1		Rcvtty Arbitrary Command Execution	Medium	CyberNotes-2000-24
BTT Software ⁸⁸	SNMP Trap Watcher Version 1.16	Windows 95/98/NT 4.0	SNMP Trap Watcher Remote Denial of Service	Low	CyberNotes 2000-04
Bytes ⁸⁹	Interactive Web Shopper 1.0, 2.0	Windows NT 4.0/2000, Unix	Interactive Web Shopper Directory Traversal	Medium	CyberNotes-2000-21

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Caldera Systems, Inc. ⁹⁰	OpenLinux 2.3	Unix	Caldera OpenLinux 2.3 rpm_query CGI Vulnerability	Medium	CyberNotes 2000-05
Caldera Systems, Inc. ⁹¹	OpenLinux Desktop 2.3	Unix	Caldera Mount/Umount Buffer Overflow	Medium	CyberNotes 2000-03
Caldera Systems, Inc. ⁹²	OpenLinux Desktop 2.3 (with linux-2.2.10-10 or lower), eServer 2.3 (with linux-2.2.14-2S or lower), eDesktop 2.4 (with Linux 2.2.14-5 or lower)	Unix	OpenLinux Setuid Applications Root Compromise	High	CyberNotes 2000-12
Caldera Systems, Inc. ⁹³	OpenLinux Desktop 2.3 , eServer 2.3 eBuilder, & eDesktop 2.4 with previous to inn-2.2.3	Unix	Caldera OpenLinux INN	Medium	CyberNotes 2000-12
Caldera Systems, Inc. ⁹⁴	OpenLinux eDesktop 2.4, OpenLinux 2.3, & OpenLinux eBuilder for Ecential 3.0	Unix	OpenLinux KDE Root Compromise	High	CyberNotes 2000-12
Carnegie Mellon University ⁹⁵	Carnegie Mellon University Cyrus-SASL 1.5.24 with RedHat 7.0	Unix	RedHat Cyrus-SASL Authorization	Medium	CyberNotes-2000-22
CatSoft ⁹⁶	Serv-U 2.4, 2.5	Windows 3.1/95/98/NT 4.0/2000	Serv-U FTP Directory Traversal	High	CyberNotes-2000-25
CatSoft ⁹⁷	Serv-U 2.5x	Windows 95/98/NT 4.0/2000	Serv-U Bruteforce	Medium	CyberNotes-2000-22
Caucho Technology ⁹⁸	Resin 1.2	Windows NT 4.0	Resin JSP Source Disclosure	Medium	CyberNotes-2000-24
Cayman ⁹⁹	3220-H DSL Router 1.0, GatorSurf 5.5Build R1, 5.5Build R0, 5.3Build R2, 5.3Build R1, GatorSurf 5.3		Cayman 3220H DSL Router "ping of death"	Low	CyberNotes 2000-11
Cayman ^{100,101}	220-H DSL Router 1.0, GatorSurf 5.5Build R0, 5.3Build R2, 5.3Build R1		DSL Router Denial of Service	Low	CyberNotes 2000-10, CyberNotes 2000-11
CGI Script Center ¹⁰²	Account Manager LITE 1.0, Account Manager PRO 1.0	Windows NT 4.0/2000, Unix	Manager LITE / PRO Administrative Password Alteration	High	CyberNotes 2000-17
CGI Script Center ¹⁰³	Auction Weaver 1.02 and previous	Windows 95/98/NT 4.0/2000, Unix	Auction Weaver Directory Traversal	Medium	CyberNotes 2000-18
CGI Script Center ¹⁰⁴	Auction Weaver 1.02 and previous	Windows 95/98/NT 4.0/2000, Unix	Auction Weaver Remote Command Execution	High	CyberNotes 2000-18
CGI Script Center ¹⁰⁵	Auction Weaver LITE 1.0, 1.01-1.04	Windows 95/98/NT 4.0/2000, Unix	Auction Weaver Multiple Vulnerabilities	Medium	CyberNotes-2000-21
CGI Script Center ¹⁰⁶	News Update 1.1		News Update Password Changing	High	CyberNotes-2000-22
CGI Script Center ¹⁰⁷	Subscribe Me Lite 2.0	Windows NT 4.0/2000, Unix	Subscribe Me LITE Administrative Password Alteration	Medium	CyberNotes 2000-17
CGI Script Center ¹⁰⁸	Subscribe Me Lite 2.0	Windows NT 4.0/2000, Unix	Subscribe-Me Lite Administration Access	Medium	CyberNotes-2000-25
CGI Script Center ¹⁰⁹	Subscribe Me Lite 2.01	Windows NT 4.0/2000, Unix	Subscribe Me Lite Account Deletion	Medium	CyberNotes-2000-23
CGI-World ¹¹⁰	Poll It 2.0		Poll It Internal Variable Override	Medium	CyberNotes 2000-14

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Check Point Software ¹¹¹	Firewall-1 3.0, 4.0		Firewall-1 Valid Username Brute Force	Medium/ High (High, if DDoS best-practices not in place)	CyberNotes-2000-23
Check Point Software ¹¹²	Firewall-1 4.0 & 4.1	Windows NT/2000	Check Point Firewall-1 IP Fragment Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-12
CheckPoint Software ¹¹³	Firewall- 1 3.0, 4.0, 4.1		Checkpoint Firewall-1 Internal Address Leakage	High	CyberNotes 2000-06
CheckPoint Software ¹¹⁴	Firewall-1 3.0, 4.0, 4.1		Firewall-1 Spoofed Source Denial of Service	Low/ High (High if DDoS best-practices not in place)	CyberNotes 2000-14
CheckPoint Software ¹¹⁵	Firewall-1 3.0, 4.0, 4.1		Firewall-1 Unauthorized RSH/REXEC Connection	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-16
Checkpoint Software ¹¹⁶	Firewall-1 4.0, 3.0		Checkpoint FireWall-1 FTP Server	High	CyberNotes 2000-03
Checkpoint Software ¹¹⁷	Firewall-1 4.0, 4.1	Windows NT	Firewall-1 Remote Resource Overload	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-14
Checkpoint Software ¹¹⁸	FW-1 3.x, 4.x		Checkpoint FW Authentication Vulnerabilities	Medium	CyberNotes 2000-02
Checkpoint Software ¹¹⁹	Firewall-1 3.0		Checkpoint Firewall-1 Script Tag Checking Bypass	High	CyberNotes 2000-03
Christopher Heschong ¹²⁰	Twig 2.5.1		Twig Remote Arbitrary Script Execution	High	CyberNotes-2000-24
Cisco Systems ¹²¹	Catalyst 4000 and 5000 images running version 4.5(2) up to 5.5(4) and 5.5(4a); Catalyst 6000 images running version 5.3(1)CSX, up to and including 5.5(4), 5.5(4a)		Cisco Catalyst Memory Leak Denial of Service	Low	CyberNotes-2000-25
Cisco Systems ¹²²	Catalyst 4000, 5000, 5500, 6000, 6500 5.4.1		Cisco Catalyst Enable Password Bypass	Medium	CyberNotes 2000-08
Cisco Systems ¹²³	Cisco Catalyst 3500 XL		Cisco Catalyst Remote Arbitrary Command Execution	High	CyberNotes-2000-22
Cisco Systems ¹²⁴	Cisco IOS 12.1(4)		Cisco IOS Extended Access List Failure	Medium	CyberNotes-2000-22
Cisco Systems ¹²⁵	Cisco IOS Software releases for the GSR starting with release 11.2(15)GS1A		Cisco Gigabit Switch Router with Fast/Gigabit Ethernet Cards ACL Bypass/Denial of Service	Medium/ High (High if DDoS best- practices not in place)	CyberNotes 2000-16
Cisco Systems ¹²⁶	Cisco IOS versions 12.0-12.1		Cisco IOS “?” HTTP Request Denial of Service	Low	CyberNotes-2000-22

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Cisco Systems ¹²⁷	DSL Router 675.0, 677.0		Cisco 675 Web Administration Denial of Service	Low	CyberNotes-2000-24
Cisco Systems ¹²⁸	IOS 9.14, 12.0.1W-12.0.7, 12.0, 12.0(5)T, 12.0(9)S, 12.0DB, 12.0S, 12.0T, 11.2-11.2.9XA, 11.1.13, 11.1.15, 11.1.16, 11.1.17, 11.1		Cisco Router Online Help	Medium/ **High	CyberNotes 2000-09
Cisco Systems ¹²⁹	PIX Firewall up to and including 4.2(5), 4.4(4), 5.0(3) and 5.1(1)		Secure PIX Firewall TCP Reset	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-14
Cisco Systems ¹³⁰	Secure ACS for Windows NT 2.42 and previous	Windows NT 4.0	Cisco Secure ACS Multiple Vulnerabilities	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-19
Cisco Systems ¹³¹	Secure PIX Firewall (versions up to and including 4.2(5), 4.4(4), 5.0(3))		Cisco Fixup Protocol FTP Vulnerabilities	High	CyberNotes 2000-06
Cisco Systems ¹³²	TACACS+ Server Developer's Kit		Cisco TACACS+ Multiple Vulnerability	High	CyberNotes 2000-11
Cisco Systems ¹³⁵	Virtual Central Office 4000 (VCO/4K) 5.1.3 and earlier		Cisco CVCO/4k Remote Username and Password Retrieval	High	CyberNotes-2000-22
Cisco Systems ^{134, 135}	IOS 11.0, 11.2x, 11.3x, 12.0x		Cisco IOS HTTP Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-09, CyberNotes 2000-10
Cisco Systems ^{136, 137}	IOS Software 11.3AA, 12.0 releases: 12.0(2) up to and including 12.0(6) and 12.0(7)		Cisco IOS Software TELNET Option Handling	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-08, CyberNotes 2000-13
Cisco Systems ^{138, 139}	PIX Firewall 4.2(5), 4.2.1, 4.2.2, 4.3, 4.4(4), 5.0-5.2		Cisco PIX Firewall SMTP Content Filtering Evasion	Medium/High (High if DDoS best-practices not in place)	CyberNotes 2000-19, CyberNotes 2000-21
Citrix ¹⁴⁰	MetaFrame for Unix 1.0; MetaFrame for Windows 2000 1.8 and earlier; MetaFrame for Windows NT 4.0 TSE 1.8 and earlier; WinFrame for Windows NT 3.5 1.8	Windows 3.5.1/NT 4.0/2000, Unix	ICA Weak Encryption	Medium	CyberNotes 2000-07
Cmail ¹⁴¹	Cmail WebMail 2.4.7	Windows NT	Cmail WebMail Denial of Service & Buffer Overflow Vulnerabilities	High	CyberNotes 2000-12
CNC Technology ¹⁴²	BizDB 1.0		BizDB bizdb-search.cgi Remote Command Execution	High	CyberNotes 2000-08
Cobalt Networks ¹⁴³	RaQ2, RaQ3 (FrontPage)		Cobalt FrontPage Vulnerability	Medium	CyberNotes 2000-11
Cobalt Networks ¹⁴⁴	RaQ 2.0, 3.0		Cobalt RaQ Apache .htaccess Disclosure	Medium	CyberNotes 2000-07
Cobalt Networks ¹⁴⁵	RaQ1, 2, 3		Cobalt RaQ Password CGI	High	CyberNotes 2000-03
Compaq ¹⁴⁶	Compaq Management Agents for Netware 2.28	Windows NT	Compaq Management Agents for Netware Plaintext Password	High	CyberNotes-2000-23
Computer Associates, Inc. ¹⁴⁷	ARCServeIT 6.63 Linux	Unix	ARCServeIT ClientAgent Temporary File	High	CyberNotes 2000-16

** High due to Phrack 55 discussion concerning Bastion routers and Phrack 56 discussion of rerouting techniques and a published tunneling script.

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Computer Associates, Inc. ¹⁴⁸	eTrust Access Control 4.1, 4.1-SP1, 5.0, 5.0-SP1	Windows NT 4.0, Unix	eTrust Access Control Default Encryption Key	High	CyberNotes 2000-17
Computer Associates, Inc. ¹⁴⁹	InoculateIT 4.53	Windows NT	InoculateIT MS Exchange Agent	Medium/High	CyberNotes-2000-23
Computer Associates, Inc. ¹⁵⁰	SessionWall-3 (AKA eTrust IDS)	Windows NT/2000	SessionWall-3 Password & Remote Discovery Vulnerabilities	Medium	CyberNotes 2000-12
Computer Power Solutions ¹⁵¹	Visual CASEL 3.0, 3.5		Visual CASEL File Name Trust	High	CyberNotes 2000-02
Concatus ¹⁵²	Imate WebMail Server 2.5	Windows NT	Imate WebMail Denial of Service	Low	CyberNotes 2000-12
Concurrent Version Systems ¹⁵³	CVS 1.10.8		CVS Multiple Vulnerabilities	Medium	CyberNotes 2000-16
Conectiva ¹⁵⁴	OpenLDAP 1.2.7, 1.2.78, 1.2.9, 1.2.10, 1.2.11	Unix	OpenLDAP UD Group Writable	Medium	CyberNotes 2000-15
Corel ¹⁵⁵	Corel Linux artCorel xconf	Unix	ArtCorel xconf Validation	High	CyberNotes 2000-05
Corel ¹⁵⁶	Linux	Unix	Corel Linux Update PATH	High	CyberNotes 2000-02
Corel ¹⁵⁷	Linux OS 1.0	Unix	Corel Linux Dosemu Distribution Configuration	High	CyberNotes 2000-05
CRYPTOCARD ¹⁵⁸	CRYPTO Admin 4.1	Multiple systems	CRYPTOCARD Weak Encryption	Medium	CyberNotes 2000-08
CS&T ¹⁵⁹	Corporate Time for the Web 2.1.2 and previous	Unix	CorporateTime for the Web Brute Force	Medium	CyberNotes-2000-23
CSM ¹⁶⁰	CSM Mail Server v2000.08-01A; 1999-07M, I, H, G		Denial of Service Vulnerability	High	CyberNotes 2000-01
CVSWeb Developer ¹⁶¹	CVSWeb 1.80	Windows NT 2000, Unix	CVSWeb Insecure Perl	High	CyberNotes 2000-15
CyberCash ¹⁶²	Merchant Connection Kit (MCK) 3.2.0.4		CyberCash Predictable Temporary File	High	CyberNotes 2000-02
Cyrus ¹⁶³	Cyrus 1.6.x	Unix	Cyrus with Postfix and Procmail Remote Shell Expansion	High	CyberNotes 2000-14
DalNet ¹⁶⁴	IRCD 4.6.5		IRCD Server 'Summon' Buffer Overflow	Medium	CyberNotes 2000-13
Daniel Beckham ¹⁶⁵	The Finger Server 0.82beta		Finger Server Pipe	High	CyberNotes 2000-03
Daniel Stenberg ¹⁶⁶	cURL prior to version 6.0-1.1; cURL-ssl prior to version 6.0-1.2; Debian GNU/Linux 2.2	Unix	cURL Remote Buffer Overflow	High	CyberNotes-2000-21
Dansie ¹⁶⁷	Shopping Cart 2.84, 3.03, 3.04	Multiple platforms	Dansie Shopping Cart Multiple Vulnerabilities	High	CyberNotes 2000-08
Danware ¹⁶⁸	NetOp 6.0. 6.50	Windows 3x/95/98/ NT 4.0/2000	NetOp Remote Control Unauthenticated File Transfer	Medium	CyberNotes 2000-11
David Harris ¹⁶⁹	Pegasus Mail 3.12	Windows 95/98/NT 4.0/2000	Pegasus E-mail File Forwarding	Medium	CyberNotes 2000-20
Davide Libenzi ¹⁷⁰	XMail 0.58		XMail Buffer Overflow	Low/High	CyberNotes 2000-18
DC Scripts ¹⁷¹	DCForum 1.0-6.0	Windows NT/2000, Unix	DCForum cgforum.cgi Arbitrary File Disclosure	High	CyberNotes-2000-23.
Debian ¹⁷²	Boa Webserver 0.94.8.2x and earlier	Unix	Boa Webserver File Disclosure	Medium	CyberNotes-2000-21
Debian ¹⁷³	CUPS 1.0.3 and prior; CUPS 1.0.5	Unix	CUPS Denial of Service	Low	CyberNotes 2000-13
Debian ¹⁷⁴	GNU/Linux 2.1	Unix	Debian Make Race Condition	Low	CyberNotes 2000-04
Debian ¹⁷⁵	Linux 2.0, 2.0r5, 2.1, 2.2, 2.2pre potato	Unix	Debian GNU/Linux MBR password bypass	Medium	CyberNotes 2000-03
Debian ¹⁷⁶	Linux 2.1	Unix	Debian APCD Symlink	High	CyberNotes 2000-03

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Debian, RedHat ^{177, 178}	NMH 1.0.2 and prior (distributed with Debian GNU/Linux 2.1, Red Hat Linux 5.2, 6.0, 6.1)	Unix	nmh Buffer Overflow	High	CyberNotes 2000-05
Debian/RedHat ¹⁷⁹	Splitvt 1.6.3	Unix	Linux Splitvt Buffer Overflow	High	CyberNotes 2000-12
Deerfield Communications ¹⁸⁰	Alt-N MDAemon 2.8.50	Windows 95/98/NT 4.0	MDAemon Denial of Service	Low	CyberNotes 2000-13
Deerfield Communications ¹⁸¹	Cat Soft Serv-U 2.5d	Windows 3.1/05/9/NT 4.0	Serv-U FTP Server Path Disclosure	Medium	CyberNotes 2000-05
Deerfield Communications ¹⁸²	FTP Serv-U 2.5e	Windows 95/9/NT 4.0/2000	FTP Serv-U Denial of Service	Low	CyberNotes 2000-16
Deerfield Communications ¹⁸³	MDAemon 3.0.3	Windows 95/98/NT 4.0/2000	MDAemon Denial of Service	Low	CyberNotes 2000-11
Deerfield Communications ¹⁸⁴	Serv-U FTP-Server v2.5b	Windows 3.1/95/98/NT 4.0	Serv-U FTP SHGetPathFromIDLst	Low	CyberNotes 2000-03
Digital (Compaq) ¹⁸⁵	TRU64/Digital Unix 4.0d, 4.0e, 4.0f, 5.0	Unix	TRU64 Digital Unix Kdebugd Remote Arbitrary File Write	High	CyberNotes 2000-19
DNSTools Software ¹⁸⁶	DNSTools 1.0.8		DNSTools Input Validation	High	CyberNotes 2000-05
E-Commerce Exchange ¹⁸⁷	Quick Commerce		Quick Commerce Insecure Transaction Process	Low	CyberNotes 2000-11
eEye Digital Security ¹⁸⁸	eEye Digital Security IRIS 1.0.1; SpyNet CaptureNet 3.0.12	Windows 95/98/98 SE/ NT 4.0/2000	eEye IRIS Buffer Overflow	Low	CyberNotes 2000-18
Element N.V. ¹⁸⁹	Element InstantShop 1.0	Windows NT 4.0	Element InstantShop Price Modification	High	CyberNotes-2000-22
Endymion ¹⁹⁰	MailMan WebMail 3.0.25 and prior	Windows, Unix	MailMan WebMail Remote Arbitrary Command Execution	High	CyberNotes-2000-25
Enhanced Software Technologies ¹⁹¹	BRU	Unix	BRU Environmental Variable	High	CyberNotes 2000-12
EType Company ¹⁹²	EServ 2.9.2 and below	Windows 95/98/NT/ 2000	EServ Denial of Service	Low	CyberNotes 2000-12
Evolvable Corporation ¹⁹³	Shambala Server 4.5	Windows 95/09/NT 4.0/2000	Shambala Server Denial of Service And Plaintext Password Storage	Medium	CyberNotes-2000-21
Extent Technologies ¹⁹⁴	RBS ISP 2.5, 2.63	Windows 95/98/NT 4.0/2000, Unix	RBS Directory Traversal	Medium	CyberNotes 2000-20
eXtropia ¹⁹⁵	WebStore 1.0, 2.0	Windows NT 4.0/2000, Unix	WebStore Directory Traversal	Medium	CyberNotes-2000-21
Faststream Technologies ¹⁹⁶	Faststream FTP++ 2.0	Windows NT 2000	Faststream FTP++ 2.0 Denial of Service	Low	CyberNotes 2000-19
Fastream Technologies ¹⁹⁷	FUR HTTP Server v1.0b	Windows NT 2000	FUR HTTP Server Denial of Service	Low	CyberNotes 2000-19
FBLI Software ¹⁹⁸	DNS PRO v5.7 for Windows NT	Windows NT	Remote Denial of Service Vulnerability	Low	CyberNotes 2000-01
FileMaker, Inc. ¹⁹⁹	FileMaker Pro 5.0	Windows NT 4.0, MacOS 8.0, 8.1, 8.5, 8.6, 9.0	FileMaker Web Companion Software Multiple Vulnerabilities	Medium	CyberNotes 2000-09
Flicks Software ²⁰⁰	Authentix 5.1c	Windows NT	Authentix Authentication	Medium	CyberNotes-2000-23
Floosietek ²⁰¹	FTGate 2.2	Windows 95/98/NT 4.0	FTGate Mail Server	Medium	CyberNotes 2000-13
Flowerfire ²⁰²	Sawmill 5.0.21	Unix	Sawmill File Access and Weak Password Encryption	Medium	CyberNotes 2000-13

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Fortech ²⁰³	Proxy+ 2.40	Windows 95/98/NT 4.0/2000	Proxy+ Telnet Gateway	High	CyberNotes 2000-13
Foundry Networks ²⁰⁴	BigIron 7.1.09; FastIron 7.1.09; ServerIron 7.1.09		Foundry Networks Telnet Login Denial of Service	Low	CyberNotes-2000-23
Foundry Networks ^{205, 206}	ServerIron 5.1.10t12, 6.0		ServerIron TCP/IP Sequence Predictability Vulnerability	High	CyberNotes 2000-05, CyberNotes 2000-06
Francisco Burzi ²⁰⁷	PHP-Nuke 1.0, 2.5	Unix	PHP-Nuke Administrative Privileges	High	CyberNotes 2000-17
FreeBSD ²⁰⁸	Apsfilter 5.4.1 and below	Unix	FreeBSD Apsfilter Filter	High	CyberNotes 2000-12
FreeBSD ²⁰⁹	DeleGate 6.0.9 and prior	Unix	DeleGate Security buffer overflow	High	CyberNotes 2000-04
FreeBSD ²¹⁰	FreeBSD 3.0-3.5, 4.0, 4.1, 5.0	Unix	FreeBSD Linux Compatibility Mode Buffer Overflow	High	CyberNotes 2000-18
FreeBSD ²¹¹	FreeBSD 3.0-3.5, 4.0, 4.0 alpha, 4.1, 5.0, 5.0 alpha	Unix	FreeBSD Malformed ELF Image Denial of Service	Low	CyberNotes 2000-18
FreeBSD ²¹²	FreeBSD 3.0-5.0 alpha	Unix	FreeBSD Eject Buffer Overflow	High	CyberNotes 2000-19
FreeBSD ²¹³	FreeBSD 3.0-3.5, 4.0, 4.0 alpha, 4.1, 4.1.1, 4.1.1-STABLE	Unix	FreeBSD Telnetd Remote Denial of Service	Low	CyberNotes-2000-23
FreeBSD ²¹⁴	FreeBSD 3.0-3.4, 4.0	Unix	FreeBSD Libedit	High	CyberNotes 2000-14
FreeBSD ²¹⁵	FreeBSD 2.2.8, 3.3, 4.0, 4.1	Unix	FreeBSD Crontab/tmp File	Medium	CyberNotes-2000-22
FreeBSD ²¹⁶	FreeBSD 2.8, 3.0, 3.3; OpenBSD 2.4, 2.5, 2.6	Unix	FreeBSD Proc Filesystem	High	CyberNotes 2000-02
FreeBSD ²¹⁷	FreeBSD 2.x, 3.x, 4.0-4.1.1	Unix	FreeBSD Weak Initial Sequence Number	Medium	CyberNotes-2000-21
FreeBSD ²¹⁸	FreeBSD 3.0-3.4	Unix	FreeBSD ASMON/ ASCPU privilege elevation	High	CyberNotes 2000-04
FreeBSD ²¹⁹	FreeBSD 3.3	Unix	Xsoldier Vulnerability	High	CyberNotes 2000-01
FreeBSD ²²⁰	FreeBSD 3.4	Unix	FreeBSD ncurses Buffer Overflow	High	CyberNotes 2000-09
FreeBSD ²²¹	FreeBSD 3.4-Stable, 4.0-Current	Unix	FreeBSD Temporary File Handling	High	CyberNotes 2000-02
FreeBSD ²²²	FreeBSD 3.5, 3.5.1, 4.0, 4.1, 4.1.1-STABLE	Unix	FreeBSD ppp deny_incoming	Medium	CyberNotes-2000-24
FreeBSD ²²³	FreeBSD 3.5, 4.0, 4.0 alpha, 4.1, 5.0, 5.0 alpha	Unix	FreeBSD Ports Brouted Installation Permission	High	CyberNotes 2000-18
FreeBSD ²²⁴	FreeBSD 3.5.1, 4.1.1	Unix	FreeBSD Netscape Buffer Overflow	High	CyberNotes-2000-23
FreeBSD ²²⁵	FreeBSD 3.x and below Libmytinfo	Unix	FreeBSD Libmytinfo Buffer Overflow	High	CyberNotes 2000-11
FreeBSD ²²⁶	FreeBSD 4.0, 4.0 alpha, 4.1, 4.1.1, 4.1.1-RELEASE	Unix	FreeBSD getnameinfo() Denial of Service	Low	CyberNotes-2000-22
FreeBSD ²²⁷	FreeBSD 4.1.1	Unix	FreeBSD fingerd File Disclosure	Medium	CyberNotes-2000-21
FreeBSD ²²⁸	FreeBSD that contains orville-write	Unix	Orville Write Root Privilege	High	CyberNotes 2000-06
FreeBSD ²²⁹	Generic-NQS versions 3.50.7 and earlier	Unix	NQS	High	CyberNotes 2000-08
FreeBSD ²³⁰	Global port, versions 3.5 through to 3.55	Unix	FreeBSD Global Htags	High	CyberNotes-2000-23
FreeBSD ²³¹	Kernel FreeBSD Alpha	Unix	FreeBSD Alpha Kernel Lacks Pseudo-Random Generator	Medium	CyberNotes 2000-12
FreeBSD ²³²	Luca Deri Ntop 1.2a7-9, 1.3.1	Unix	Linux Ntop -w Buffer Overflow	High	CyberNotes 2000-17
FreeBSD ²³³	Mopd	Unix	FreeBSD Mopd Port Remote Root Compromise	High	CyberNotes 2000-18
FreeBSD ²³⁴	MySQL	Unix	MySQL Password Authentication	Medium	CyberNotes 2000-05
FreeBSD ²³⁵	Pine 4.20, 4.21; imap 4.7b, 4.7c	Unix	Pine C-client Denial of Service	Low	CyberNotes 2000-19

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
FreeBSD ²³⁶	Qopper port version 2.53 and earlier	Unix	FreeBSD Qopper String Formatting	High	CyberNotes 2000-14
FreeBSD ²³⁷	SSH installation between January 14, 2000 and April 21, 2000	Unix	FreeBSD SSH Extra Port Listening	Medium	CyberNotes 2000-12
FreeBSD ²³⁸	FreeBSD 4.0 (healthd 0.1-0.3)	Unix	Healthd Buffer Overflow	High	CyberNotes 2000-08
FreeBSD ^{239, 240}	FreeBSD 3.5x, 4.0, 4.0 alpha, 4.1, 4.1.1, 4.1.1-STABLE, RELEASE	Unix	FreeBSD top Format String	High	CyberNotes-2000-22, CyberNotes-2000-23
FreeBSD/ OpenBSD ²⁴¹	FreeBSD 2.8, 3.0, 3.3; OpenBSD 2.4, 2.5, 2.6	Unix	FreeBSD/ OpenBSD Procs Security	High	CyberNotes 2000-03
FTPPro ²⁴²	FTPPro v7.5		Insecure Registration Storage Vulnerability	High	CyberNotes 2000-01
FTPx ²⁴³	FTP Explorer 1.0.00.10		FTPx FTP Explorer Weak Password Encryption	Medium/Low	CyberNotes 2000-04
GAMSoft ²⁴⁴	Telsrv 1.4, 1.5	Windows 95/98/NT 4.0/2000	Telsrv Denial of Service	Low	CyberNotes 2000-15
GeoCel International ²⁴⁵	WindMail 3.0	Windows 95/98/NT 4.0	GeoCel WindMail Remote File Read	High	CyberNotes 2000-07
George Burgyan ²⁴⁶	CGI Counter 4.0.2, 4.0.7		CGI Counter Input Validation	High	CyberNotes 2000-10
GIFtpd ²⁴⁷	GIFtpd 1.18-1.21b8		GIFtpd Privpath Directive	Medium	CyberNotes 2000-13
GlobalScale, Inc. ²⁴⁸	CuteFTP		Password Storage Insecurity	Medium	CyberNotes 2000-01
GNU ²⁴⁹	Glibc 2.0, 2.1, 2.1.1, 2.1.1-6, 2.1.2, 2.1.3	Unix	Glib Unsetenv() Duplicate Entry Removal	Medium	CyberNotes 2000-18
GNU ²⁵⁰	glibc 2.1.3-10	Unix	Glibc Symlink	Medium	CyberNotes 2000-20
GNU ²⁵¹	GNU Cengine 1.5x, 1.5.3-4, 1.6a10	Unix	GNU Cengine Format String Vulnerabilities	High	CyberNotes 2000-20
GNU ²⁵²	Mailman prior to 1.2beta	Unix	Mailman External Archive	Medium	CyberNotes 2000-19
GNU ²⁵³	Usvrv 1.0.0	Unix	Usvrv Service Program Environment Corruption	Medium	CyberNotes 2000-16
GnuPG ²⁵⁴	GnuPG 1.0-1.0.3		GnuPG Multiple Signed Message Modification	Medium	CyberNotes-2000-21
GoodTech ²⁵⁵	FTP Server 95/98 3.0, 95/98 3.0.1 NT/2000 3.0	Windows 95/98/NT 4.0/2000	FTP Server RNTD Denial of Service	Low	CyberNotes 2000-18
Gordano ²⁵⁶	NTMail 5.0, 6.0	Windows NT 4.0/2000	NTMail Web Configuration Denial of Service	Low	CyberNotes 2000-18
Great Circle Associates ²⁵⁷	Majordomo 1.94.4, 1.94.5		Majordomo Config-file admin_password Configuration	High	CyberNotes-2000-25
Great Circle Associates ²⁵⁸	Majordomo v1.94.4		Privilege Elevation Vulnerabilities	High	CyberNotes 2000-01
GSX ²⁵⁹	gsx-0.90d gsx-0.90e		GSX Denial of Service	Low	CyberNotes-2000-23
GWScripts ²⁶⁰	News Publisher 1.05, 1.05a, 1.05b, 1.06	Windows NT, Unix	News Publisher Author.file Write	Medium	CyberNotes 2000-18
H. Nomura ²⁶¹	Tiny FTPDaemon 0.52		Tiny FTPd Buffer Overflow	High	CyberNotes 2000-03
Handspring ²⁶²	Visor Network HotSync 1.0		Authentication Vulnerability	High	CyberNotes 2000-01
Helix Code ²⁶³	GNOME Installer 0.2	Unix	Gnome Installer System Configfile Overwrite	High	CyberNotes 2000-17
Helix Code ²⁶⁴	Go-Gnome Pre-Installer 1.	Unix	Helix Code "go-gnome" /tmp Symlink	High	CyberNotes 2000-18
Hewlett-Packard ²⁶⁵	EMS A.03.00	Unix	EMS Arbitrary File Permission Change	High	CyberNotes-2000-24
Hewlett-Packard ²⁶⁶	Hewlett-Packard Web JetAdmin Version 5.6	Windows NT 4.0/2000, Unix	HP Web JetAdmin Directory Traversal Vulnerability	Medium	CyberNotes 2000-11
Hewlett-Packard ²⁶⁷	Hewlett-Packard Web JetAdmin Version 6.0	Windows NT 4.0/2000, Unix	HP Web JetAdmin Remote Denial of Service	Low	CyberNotes 2000-11
Hewlett-Packard ²⁶⁸	HP OpenView Network Node Manager 6.1	Windows NT/2000	HP OpenView Network Node Manager Buffer Overflow	High	CyberNotes 2000-12
Hewlett-Packard ²⁶⁹	HP-9000 Series 700/800 running release HP-UX 11x	Unix	Trusted Systems Password	Medium	CyberNotes 2000-04

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Hewlett-Packard ²⁷⁰	HP9000 systems running HP-UX 10.10, 10.20, 10.24, 11.00, 11.04	Unix	HP-UX Dterm Privilege Elevation	Medium	CyberNotes-2000-23
Hewlett-Packard ²⁷¹	HP-UX 9.x-11.0	Unix	HP-UX Buffer Overflow	High	CyberNotes-2000-23
Hewlett-Packard ²⁷²	HP-UX 10.0.1, 10.10, 10.20, 10.24, 11.0, 11.4	Unix	HP-UX auto_parms Arbitrary Command Execution	High	CyberNotes-2000-23
Hewlett-Packard ²⁷³	HP-UX 10.20	Unix	HP-UX Registrar Local Arbitrary File Read	Medium	CyberNotes-2000-23
Hewlett-Packard ²⁷⁴	HPUX 10.20 & 11.00	Unix	HPUX Man	Medium	CyberNotes 2000-12
Hewlett-Packard ²⁷⁵	HP-UX 10.20, 11.00	Unix	HP Automountd	High	CyberNotes 2000-09
Hewlett-Packard ²⁷⁶	HP-UX 10.20, 11.00	Unix	HP-UX Crontab/tmp File	Medium	CyberNotes-2000-22
Hewlett-Packard ²⁷⁷	HP-UX 11.0	Unix	HP-UX Buffer Overflow	Low	CyberNotes 2000-16
Hewlett-Packard ²⁷⁸	HP-UX 11.	Unix	HPUX Newgrp(1)	Medium	CyberNotes 2000-17
Hewlett-Packard ²⁷⁹	HP-UX 11.0, 11.11	Unix	HP-UX MC/Service Guard Default Permissions	Low	CyberNotes-2000-23
Hewlett-Packard ²⁸⁰	HP-UX 11.4; VirtualVault 3.50	Unix	HP VirtualVault Aliased IP Addresses	Medium	CyberNotes 2000-07
Hewlett-Packard ²⁸¹	JetDirect J3111A rev. A.08.06, G.05.35, G.07.02, G.07.03, G.07.17, G.08.03, JetDirect rev. G.08.04, G.08.20, H.08.05, H.08.20		HP JetDirect Invalid FTP Command Denial of Service	Low	CyberNotes 2000-15
Hewlett-Packard ²⁸²	JetDirect J3111A rev. G.08.03, G.07.17, G.07.03, A.08.06		JetDirect Portscan Denial of Service	Low	CyberNotes 2000-08
Hewlett-Packard ²⁸³	JetDirect x.08.04, x.08.05, x.08.20		JetDirect Multiple Denial of Service Vulnerabilities	Low	CyberNotes-2000-21
Hewlett-Packard ²⁸⁴	MPE/iX 4.5, 5.0, 5.5, 6.0, 6.5	Unix	HP TurboIMAGE DBUTIL Privilege Elevation	Medium	CyberNotes 2000-13
Hewlett-Packard ²⁸⁵	OpenView Network Node Manager 4.11 HP-UX, Solaris, 5.01 HP-UX, Solaris, 6.1	Windows NT 4.x/2000, Unix	OpenView Network Node Manager Ovalarmsrv	Low	CyberNotes 2000-20
Hewlett-Packard ²⁸⁶	OpenView Network Node Manager 4.11 Solaris, HP-UX, 5.01 HP-UX, Solaris, 6.1 HP-UX 10.X, 11.X, Solaris	Unix	OpenView Network Node Manager Config Scripts	Medium	CyberNotes 2000-19
Hewlett-Packard ²⁸⁷	OpenView Network Node Manager 6.1	Windows NT 4/0/2000, Unix	OpenView Network Node Manager Web Password	Medium	CyberNotes 2000-17
Hewlett-Packard ²⁸⁸	OpenView Network Node Manager 6.1	Windows NT 4.0/2000, Unix	OpenView Node Manager SNMP Denial of Service	High	CyberNotes 2000-20
Hewlett-Packard ²⁸⁹	OpenView OmniBack II 2.55, 3.0, 3.1	Windows NT 3.5.1/4.0/2000	HP OpenView OmniBack Denial of Service	Low	CyberNotes 2000-05
Hewlett-Packard ²⁹⁰	SNMP Daemon HPUX 11.00	Unix	HPUX SNMP Daemon Temporary File Root Compromise	High	CyberNotes 2000-12
Hewlett-Packard ²⁹¹	VirtualVault 3.50, 4.0	Unix	VirtualVault Denial of Service	Low	CyberNotes-2000-22
Hewlett-Packard ²⁹²	HP9000 Series 7/800 running HP-UX 10.x, 11.x	Unix	Multiple Aserver Vulnerabilities	High	CyberNotes 2000-01
Hewlett-Packard ^{293, 294}	HP9000 series 7/800 servers running HP-UX release 11.00	Unix	Multiple Wu-Ftp Vulnerabilities	High	CyberNotes 2000-02
Hewlett-Packard ^{295, 296}	HP-UX 11.0, 10.30	Unix	PMTU Denial of Service	Low	CyberNotes 2000-02, CyberNotes 2000-04
Hewlett-Packard; Sun Microsystems ²⁹⁷	UP-UX 10.1, 10.20; Solaris 2.5, 2.5.1, 2.6	Unix	Local Privilege Elevation Vulnerability	Medium	CyberNotes 2000-01
Horde ²⁹⁸	Horde 1.2	Unix	Horde CGI Remote Command Execution	High	CyberNotes 2000-19

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Horde ²⁹⁹	IMP 2.0, 2.2		IMP File Disclosure	Medium	CyberNotes 2000-19
Hughes Technology ³⁰⁰	MiniSQL v2.0.4.1 through 2.0.11		Remote CGI Buffer Overflow Vulnerability	High	CyberNotes 2000-01
IBM ³⁰¹	AIX 3.2.x, 4.1.x, 4.2.x, 4.3.x	Unix	AIX Locale Subsystem Format String	High	CyberNotes-2000-23
IBM ³⁰²	AIX 4.{3,2}.x	Unix	AIX Multiple Buffer Overflow Vulnerabilities	High	CyberNotes-2000-25
IBM ³⁰³	AIX 4.1-4.1.5, 4.2, 4.2.1, 4.3-4.3.2	Unix	AIX Link Behavior	High	CyberNotes 2000-06
IBM ³⁰⁴	AIX 4.3, 4.3.1, 4.3.2	Unix	AIX Cdmount Insecure External Program Call	High	CyberNotes 2000-13
IBM ³⁰⁵	AIX 4.3., 4.3.1, 4.3.2	Unix	AIX frctrll Insecure File Handling	High	CyberNotes 2000-09
IBM ³⁰⁶	DB2 Universal Database for Linux 6.1; DB2 Universal Database for Windows NT 6.1	Windows NT 4.0/2000, Unix	DB2 Universal Database Known Default Password	High	CyberNotes-2000-25
IBM ³⁰⁷	DB2 Universal Database for Windows NT 6.1, 7.1	Windows NT 4.0/2000	DB2 Universal Database for Windows NT SQL Denial of Service	Low	CyberNotes-2000-25
IBM ³⁰⁸	HTTP Server 1.3.6.3	Windows NT, Unix	HTTP Server Denial of Service	Low	CyberNotes-2000-24
IBM ³⁰⁹	IBMHSSSB 1.0	Unix	IBM Ikeyman Java Class Creation Vulnerability	High	CyberNotes 2000-07
IBM ³¹⁰	Lotus Domino	Windows NT 4.0, Unix	Domino Remote Document Modification	Low	CyberNotes 2000-11
IBM ³¹¹	Lotus Domino 5.0.1	Windows NT 4.0, Unix	Domino Remote SMTP Buffer Overflow	High	CyberNotes 2000-11
IBM ³¹²	Net.Data 7.0	Windows NT 4.0, OS/2, OS/390, OS/400, Unix	Net.Data Path Disclosure	Medium	CyberNotes-2000-24
IBM ³¹³	Net.Data db2www	Windows NT, Unix, OS2	Net.Data db2www Buffer Overflow	High	CyberNotes 2000-19
IBM ³¹⁴	NetStation Manager		Race Condition Vulnerability	High	CyberNotes 2000-01
IBM ³¹⁵	OS/2 FTP Server 4.0, 4.2, 4.3		OS/2 FTP Server Login Denial of Service	Low	CyberNotes 2000-17
IBM ³¹⁶	WebSphere 3.0.2	Windows NT, Unix	IBM WebSphere Showcode	Medium	CyberNotes 2000-15
IBM ³¹⁷	WebSphere Application Server 3.0.2	Windows NT 4.0, Unix	WebSphere Application Server Plugin Denial of Service	Low	CyberNotes 2000-19
ICQ ³¹⁸	ICQ 2000a ICQ 99a & 99b with ICQ WebFront enabled		ICQ Guest Book Buffer Overflow	High	CyberNotes 2000-12
ICQ ³¹⁹	ICQ 2000a		ICQ 2000a ICQmail Temporary Internet Link	Medium	CyberNotes 2000-12
ICRadius ³²⁰	ICRADIUS 0.14		IC Radius Buffer Overflow	High	CyberNotes 2000-09
Id Software Inc. ³²¹	Quake3 Arena 1.16n	Windows 95/98/NT 4.0	id Software Quake3Arena Directory Traversal	MediumHigh (High if network security best-practices not in place)	CyberNotes 2000-09
i-drive.com ³²²	Filo 1.0.0.1	Windows NT	i-drive Filo Remote Buffer Overflow	High	CyberNotes 2000-12
Imatix ³²³	Xitami Webserver		Xitami Webserver Denial of Service	Low	CyberNotes 2000-07
iMesh.Com ³²⁴	iMesh 1.02 and previous	Windows 95/98/NT 4.0/2000	iMesh Buffer Overflow	High	CyberNotes 2000-13
IMP ³²⁵	IMP 2.0.11		IMP 2 Vulnerabilities	Medium	CyberNotes 2000-09
Infonautics ³²⁶	Infonautics applications		Infonautics Getdoc.cgi Access	High	CyberNotes 2000-08

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Infopop Corp. ³²⁷	Ultimate Bulletin Board 5.43		Ultimate Bulletin Board Perl CGI Security Vulnerability	High	CyberNotes 2000-04
Infopulse ³²⁸	GateKeeper 3.5 and previous	Windows 95/98/NT 4.0/2000	Gatekeeper Buffer Overflow	High	CyberNotes 2000-15
Inktomi (formerly known as Infoseek) ³²⁹	Ultraseek Server 3.0	Windows NT 4.0, Unix	Ultraseek Information and Source Disclosure Vulnerabilities	Medium	CyberNotes-2000-25
Inktomi Search Software ³³⁰	Inktomi Search Software 3.x	Windows NT4.0, Unix	Inktomi Search Software Denial of Service	Low	CyberNotes-2000-22
Intel Corporation ³³¹	Express 510T, 520T, 550F, 550T (Firmware 2.63 & 2.64)		Express Switch 500 Series Malformed ICMP Packet Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-18
Intel Corporation ³³²	Express 550F (Firmware 2.63 2.64)		Express Switch 500 Series Denial of Service	Low	CyberNotes 2000-18
Intel Corporation ³³³	InBusiness E-mail Station v1.04 and prior		E-mail Station Security Vulnerability (TCP244)	High	CyberNotes 2000-01
Intel Corporation ³³⁴	InBusiness eMail Station 1.4.87		Intel InBusiness eMail Station Denial of Service	Low/High	CyberNotes-2000-22.
Intel Corporation ³³⁵	NetStructure 7180.0, 7110.0		NetStructure Undocumented Password and Remote Backdoor	High	CyberNotes 2000-10
Inter7 ³³⁶	Vpopmail (vchkw) prior to 4.8		Vpopmail Format String Via User Input	High	CyberNotes 2000-14
Inter7 ³³⁷	Vpopmail (vchkw) 3.4.1 through 3.4.11		Inter7 Vpopmail Buffer Overflow	High	CyberNotes 2000-02
International TeleCommunications ^{338, 339}	WebBBS 1.1.5	Windows NT 4.0	WebBBS Web Server Buffer Overflow	High	CyberNotes 2000-13, CyberNotes 2000-14
Internet Security Systems ³⁴⁰	RealSecure 3.0, 3.1, 3.2, 3.2.1999	Windows NT 4.0	RealSecure CGI and Denial of Service Attack Subversion	Low	CyberNotes 2000-05
Internet Security Systems ³⁴¹	RealSecure 3.2.1, 3.2.2	Windows NT, Unix	RealSecure Fragmented SYN Packets Denial of Service	Low	CyberNotes 2000-17
Internet Software Consortium (ISC) ³⁴²	Bind 8.2-8.2.2, 4.9.7-T1B, 4.9.7, 8.1-8.1.2; Multiple DNS Servers	Unix	Nameserver Traffic Amplification and NS Route Discovery	Low	CyberNotes 2000-04
iPlanet ³⁴³	Web Server Enterprise Edition 4.1		iPlanet Denial of Service	Low	CyberNotes 2000-05
IPSwitch ³⁴⁴	IMail 5.0-5.0.8, 6.0	Windows NT 3.5.1/4.0	Password Encryption Scheme Vulnerability	Medium	CyberNotes 2000-01
IPSwitch ³⁴⁵	IMail 6.00, 6.01, 6.02	Windows NT 3.5.1/4.0	IMail Web Service Remote Denial of Service	Low	CyberNotes 2000-17
IPSwitch ³⁴⁶	IMail 6.0-6.4	Windows NT 3.5.1/4.0/2000	IMail File Attachment	Medium	CyberNotes 2000-18
IPSwitch ³⁴⁷	IMonitor Server 5.08 and prior	Windows NT 3.5.1/4.0	Denial of Service Vulnerability	Low	CyberNotes 2000-01
IPSwitch ³⁴⁸	IMail 5.0, 5.0.5-5.0.8, 6.0- 6.2	Windows NT 3.5.1/4.0/2000	IMail Server Authentication Denial of Service	Low	CyberNotes 2000-07
IPSwitch ³⁴⁹	IMail 6.0.5	Windows NT 4.0/2000	IMail Denial of Service	Low	CyberNotes-2000-25
IPSwitch ³⁵⁰	WinCOM LPD 1.00.90	Windows 95/98/NT 4.0	WinCOM LPD Denial of Service	Low	CyberNotes 2000-19
ITAfrica ³⁵¹	WEBactive 1.0	Windows 95/98/NT 4.0/2000	WEBactive HTTP Server Long GET Request	Low	CyberNotes 2000-15
ITHouse ³⁵²	ITHouse Mail Server	Windows NT	ITHouse Mail Server Denial of Service	High	CyberNotes 2000-12
ITHouse ³⁵³	ITHouse Mail Server 1.0.4	Windows 3.51/95/NT 4.0	ITHouse Mail Server 1.04 Buffer Overflow	High	CyberNotes 2000-11
Jack De Winter ³⁵⁴	WinSMTP 1.6f, 2.x	Windows 95/98/NT 4.0	WinSMTP Buffer Overflow	High	CyberNotes 2000-19
JCServ.News ³⁵⁵	MultiHTML version 2.2		MultiHTML Local File Retriever	Medium	CyberNotes 2000-19
Joshua Chamas ³⁵⁶	Apache::ASP ASP 0.16-0.18, 1.93		Apache::ASP Source.asp Example Script	High	CyberNotes 2000-14

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
KDE ³⁵⁷	kvt 1.1.2	Unix	Kvt Format String	High	CyberNotes 2000-19
KDE ^{358, 359}	KDE 1.1, 1.1.1, 1.2, 2.0 BETA	Unix	KDE Kscd SHELL Environmental Variable	High	CyberNotes 2000-10, CyberNotes 2000-11
Kevin Lindsay ³⁶⁰	Secure Locate 1.4-1.6, 2.0-2.2	Unix	Secure Locate Heap Corruption	High	CyberNotes-2000-24
Keware Technologies ³⁶¹	HomeSeer 1.4	Windows 95/98/NT 4.0/2000	HomeSeer Directory Traversal	High	CyberNotes-2000-25
Khalim Landross ³⁶²	EFTP 2.0.4.281		EFTP Buffer Overflow	High	CyberNotes 2000-19
Kirk Bauer ³⁶³	DiskCheck 3.1.1 DiskCheck is included with RedHat "Rawhide" and "Pinstripe".	Unix	DiskCheck Race Condition	High	CyberNotes 2000-16
Kootenay Web Inc. ³⁶⁴	whois 1.0	Unix	Whois Remote Command Execution	High	CyberNotes-2000-22
Krzysztof Dabrowski ³⁶⁵	cmd5checkpw 0.20, 0.21		cmd5checkpw Qmail Remote Password Retrieval	Medium	CyberNotes-2000-21
KTH (Royal Institute of Technology, Sweden) ³⁶⁶	Kerberos 4 1.0.3-1.0 and prior	Unix	Multiple Kerberos Vulnerabilities	High	CyberNotes-2000-25
Lawrence Berkeley Laboratory ³⁶⁷	Tcpdump 3.4-3.5	Unix	Tcpdump DNS Decode	High	CyberNotes 2000-09
Lawrence Berkeley Laboratory ^{368, 369}	tcpdump 3.4, 3.5, 3.5 alpha	Unix	tcpdump Packet Buffer Overflow	High	CyberNotes-2000-22, CyberNotes-2000-23
Leif M. Wright ³⁷⁰	Everything form.cgi 2.0		everythingform.cgi Arbitrary Command Execution	High	CyberNotes-2000-25
Leif M. Wright ³⁷¹	simplestguest.cgi 2.0		Simplest-guest.cgi Remote Command Execution	High	CyberNotes-2000-25
Leif M. Wright ³⁷²	simplestmail.cgi 1.0		simplestmail.cgi Remote Command Execution	High	CyberNotes-2000-25
LIDS ³⁷³	LIDS 0.9.7	Unix	LIDS Root Level Access When Disabled	High	CyberNotes 2000-16
Lilikoi Software, Inc. ³⁷⁴	Ceilidh 2.60a	Windows NT	Ceilidh Denial of Service & Path Revealing Vulnerabilities	Low/ Medium	CyberNotes 2000-12
Linux ³⁷⁵	Halloween 4 Linux Power Tools CD, (any system that has atsar-linux-1.4.2)	Unix	Atsadc Local Root Compromise	High	CyberNotes 2000-06
Linux and BSD ³⁷⁶	Linuxconf	Unix	Buffer Overflow Vulnerability	High	CyberNotes 2000-01
Lotus Development Corporation ³⁷⁷	Domino Mail Server 5.0.1-5.0.4, Domino Enterprise Server 5.0.1-5.0.4	Windows NT 4.0, Unix	Domino SMTP Server ENVID Buffer Overflow & Denial of Service	High	CyberNotes-2000-23
Lotus Development Corporation ³⁷⁸	Lotus Notes Client 5.0-5.0.5		Lotus Notes S/MIME	Medium	CyberNotes-2000-23
Lotus Development Corporation ³⁷⁹	Lotus Notes Client R5		Lotus Notes Client R5 File Existence Verification	Medium	CyberNotes-2000-24
Lotus Development Corporation ³⁸⁰	LotusNotes v4.6.1		Cgi-Bin Vulnerabilities	Low	CyberNotes 2000-01
L-Soft ³⁸¹	Listserv 1.8c, 1.8d	Windows 9x/2000/ NT 3.5x/4.0, Unix, OpenVMS VAX	Listserv Web Archives Long QUERY_ STRING Buffer Overflow	High	CyberNotes 2000-15
MandrakeSoft ³⁸²	Linux Mandrake 6.0, 6.2, 7.0, 7.1	Unix	Linux-Mandrake Update Race Condition	Medium	CyberNotes 2000-17
MandrakeSoft ³⁸³	Linux Mandrake 7.0, 7.1	Unix	Mandrake XSession Local Xauthority Bypass	Medium	CyberNotes 2000-20
MandrakeSoft ³⁸⁴	Mandrake 6.1, 7.0, 7.1	Unix	Mandrake /perl http Directory Disclosure	Medium	CyberNotes 2000-19
MandrakeSoft RedHat ³⁸⁵	MandrakeSoft Linux Mandrake 7.0; RedHat Linux 6.1, 6.2	Unix	Printtool Config File Permissions	Medium	CyberNotes 2000-05

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
MandrakeSoft ³⁸⁶	Mandrake 7.02 Kdesud	Unix	Mandrake Kdesud Buffer Overflow	High	CyberNotes 2000-11
MandrakeSoft Linux ³⁸⁷	Mandrake 7.1	Unix	Linux Usermode Package	Low	CyberNotes 2000-15
MandrakeSoft ^{388, 389}	Mandrake 6.1, 7.0	Unix	Linux cdrecord Buffer Overflow	High	CyberNotes 2000-11, CyberNotes 2000-12
MandrakeSoft, RedHat, SuSE ³⁹⁰	RedHat Linux 5.1, 5.2, 6.0, 6.1, 6.2; Linux Mandrake 6.1, 7.0; SuSE 6.2	Unix	Linux "dump" Buffer Overflow	High	CyberNotes 2000-05
Markus Triska ³⁹¹	CGIForum 1.0		CGIForum Arbitrary File Disclosure	Medium	CyberNotes-2000-24
Martin K. Peterson ³⁹²	gdm 2.0.x BETA + GNOME, GNOME 1.0.x, gdm 1.0.x+ GNOME, GNOME 1.0.x	Unix	GNOME gdm XDMCP Buffer Overflow	High	CyberNotes 2000-11
Matt Wright ³⁹³	FormMail 1.6	Unix	FormMail Environmental Variables Disclosure	Medium	CyberNotes 2000-10
Matthew Redman ³⁹⁴	Allmanage 2.6		Allmanage Administrator Password Retrieval	Medium	CyberNotes 2000-10
Max Feoktistov ³⁹⁵	Small HTTP server 2.01	Windows 95/98	Small HTTP Server Multiple Denial of Service Vulnerabilities	Low	CyberNotes-2000-23
McAfee ³⁹⁶	VirusScan 4.5	Windows 95/98/ME/NT 4.0/2000	VirusScan Unquoted ImagePath	High	CyberNotes-2000-23
McMurtrey/ Whitaker & Associates, Inc. ³⁹⁷	Cart32 2.6, 3.0	Win32-based servers	Cart32 Remote Administration Password	High	CyberNotes 2000-09
McMurtrey/ Whitaker & Associates, Inc. ³⁹⁸	Cart32 (Verified in versions 2.5a and 3.0)		Cart32 Insecure Transaction Process	Medium	CyberNotes 2000-11
McMurtrey/ Whitaker & Associates, Inc. ³⁹⁹	Cart32 3.0, 3.1, 3.5		Cart32 Multiple Vulnerabilities	Low/High	CyberNotes-2000-23
Mechfire ⁴⁰⁰	WarFTP Daemon v1.7 and 1.67b2		Multiple Vulnerabilities	High	CyberNotes 2000-01
Mechfire ⁴⁰¹	WarFTPD 1.67-3, 1.66x4s		War-FTPD CWD/MKD Denial of Service	Low	CyberNotes 2000-03
Mediahouse Software ⁴⁰²	Statistics Server LiveStats 5.02	Windows NT 4.0	Statistics Server LiveStats Buffer Overflow	Medium	CyberNotes 2000-17
Mendel Cooper ⁴⁰³	Shred 1.0	Unix	Shred File Wiper Insecure File Deletion	Low	CyberNotes-2000-21
MetaProducts ⁴⁰⁴	Offline Explorer 1.0x, 1.1x, 1.2x, 1.3x		Offline Explorer File System Disclosure	Medium	CyberNotes-2000-25
MetaProducts ⁴⁰⁵	Offline Explorer 1.1	Windows 95/98/NT 4.0/2000	Offline Explorer Directory Traversal Vulnerability	Medium	CyberNotes 2000-11
Michael A. Gumienny ⁴⁰⁶	FCheck 2.7.45		FCheck Shell Metacharacter Filename	High	CyberNotes 2000-07
Microsoft ⁴⁰⁷	Windows NT 4.0 SP1-SP6	Windows NT 4.0	NT LsaQueryInformationPolicy() Domain SID Leak	Medium	CyberNotes 2000-03
Microsoft ⁴⁰⁸	Access 2000, Word 2000,	Windows 95/98/NT 4.0/2000	Microsoft Office 2000 Mail Merge	High	CyberNotes 2000-16
Microsoft ⁴⁰⁹	Access 2000, Excel 2000, FrontPage 2000, Office 2000, Outlook 2000, PowerPoint 2000, Photodraw 2000.1, Project 2000, Works 2000	Windows 95/98 NT 4.0/2000	Office 2000 UA Control	Medium	CyberNotes 2000-10
Microsoft ⁴¹⁰	Active Movie Control 1.0	Windows 95/98/NT 4.0/2000	Active Movie Control Filetype	Medium	CyberNotes 2000-10

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Microsoft ⁴¹¹	Clip Art 1.0	Windows 95/98/NT 4.0/2000	Microsoft Clip Art Buffer Overflow	High	CyberNotes 2000-05
Microsoft ⁴¹²	Commercial Internet System 2.0, 2.5; IIS 4.0, 5.0; Proxy Server 2.0; Site Server 3.0 Commerce Edition; Site Server 3.0; Commercial Internet System 2.0; BackOffice 4.0, 4.5	Windows NT 4.0/2000	Microsoft Virtualized UNC Share	Medium	CyberNotes 2000-07
Microsoft ⁴¹³	Converter Pack 2000; Office & PowerPoint 97/2000 & Word 97/98/2000 Korean, Japanese, Chinese versions	Windows 95/98/NT 4.0/2000	East Asian Word Conversion	High	CyberNotes 2000-02
Microsoft ⁴¹⁴	Data Engine 1.0, 2000; SQL Server 7.0, 2000	Windows 95/98/NT 4.0/2000	Microsoft Extended Stored Procedure Parameter Parsing	High	CyberNotes-2000-25
Microsoft ⁴¹⁵	Enterprise Manager for SQL Server 7.0	Windows NT 4.0	SQL Login ID Encryption	High	CyberNotes 2000-06
Microsoft ⁴¹⁶	Excel 2000, PowerPoint 2000, Word 2000	Windows 95/98/NT 4.0/2000	Microsoft Office HTML Object Tag	High	CyberNotes 2000-16
Microsoft ⁴¹⁷	Excel 97/2000	Windows 95/98/NT 4.0/2000	Microsoft Excel XML	Low	CyberNotes 2000-07
Microsoft ⁴¹⁸	Exchange 2000 Server CDs (without "Rev. A" stamped on the CD on the line below the Part No.); Exchange 2000 Enterprise Server CDs (without "Rev. A" stamped on the CD below the Part No.)	Windows NT 2000	Microsoft 2000 Exchange User Account	Medium	CyberNotes-2000-23
Microsoft ⁴¹⁹	FrontPage	Windows 95/98 NT 4.0	FrontPage htmimage.exe Buffer Overflow	High	CyberNotes 2000-08
Microsoft ⁴²⁰	FrontPage 2000 Server Extensions 1.1	Windows 95/98/NT 4.0/2000	FrontPage Server Extensions MS-DOS Device Name Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-17
Microsoft ⁴²¹	FrontPage 2000 Server Extensions 1.1 and previous	Windows 95/98/NT 4.0/2000	FrontPage Server Extensions Denial of Service & Path Disclosure	Low/ Medium	CyberNotes 2000-14
Microsoft ⁴²²	FrontPage 98/2000	Windows 98/2000	MS FrontPage System Information	Medium	CyberNotes 2000-03
Microsoft ⁴²³	FrontPage Personal WebServer 3.0.2.926	Windows 95/98/NT 4.0	Microsoft FrontPage PWS Directory Traversal	Medium	CyberNotes 2000-04
Microsoft ⁴²⁴	HotMail	Windows 95/98/NT 4.0/2000	JavaScript Vulnerability	High	CyberNotes 2000-01
Microsoft ⁴²⁵	Hotmail	Windows 95/98/NT 4.0/2000	Hotmail JavaScript Attachment	Medium	CyberNotes 2000-10
Microsoft ⁴²⁶	IIS 5.0, 4.0, 3.0	Windows NT 4.0/2000	NT IIS ASP VBScript Runtime Error Viewable Source	High	CyberNotes 2000-03
Microsoft ⁴²⁷	Index Server 2.0	Windows NT 4.0	MS Index Server '%20' ASP Source Disclosure Vulnerability	Medium	CyberNotes 2000-07
Microsoft ⁴²⁸	Indexing Services for Windows 2000	Windows NT 2000	Microsoft Indexing Services Cross Site Scripting	Medium	CyberNotes-2000-22
Microsoft ⁴²⁹	Indexing Services for Windows 2000	Windows NT 2000	Indexing Services for Windows 2000 File Verification	Medium	CyberNotes-2000-23
Microsoft ⁴³⁰	Internet Explorer 3.x, 4.x, 5.0	Windows 95/98/NT 4.0	Internet Explorer Cookie Disclosure	Low	CyberNotes 2000-10

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Microsoft ⁴³¹	Internet Explorer 4.0, 4.01, 5.01	Windows 95/98/NT 4.0/2000	Image Source Redirect	Medium	CyberNotes 2000-04
Microsoft ⁴³²	Internet Explorer 4.0, 4.01, 5.0, 5.01	Windows 95/98/NT	ActiveX Setup Download	Medium	CyberNotes 2000-14
Microsoft ⁴³³	Internet Explorer 4.0, 5.0, 5.01	Windows 95/98/NT/2000	Internet Explorer Cross-Frame Security Vulnerability Using IFRAME & WebBrowser	Medium	CyberNotes 2000-12
Microsoft ⁴³⁴	Internet Explorer 4.0, 5.0, 5.01, 5.5 preview	Windows 3.1/95/98/NT 3.51, 4.0, 2000	Frame Document Verification	Medium	CyberNotes 2000-10
Microsoft ⁴³⁵	Internet Explorer 4.0, 5.0, 5.01, 5.5 preview	Windows 3.1/95/98/NT 3.51, 4.0, 2000	Malformed Component Attribute	Medium	CyberNotes 2000-10
Microsoft ⁴³⁶	Internet Explorer 4.01, 4.01, 5.0, 5.01	Windows 95/98/NT/ 2000, Mac OS	Microsoft SSL Certificate Vulnerabilities	Low/Medium	CyberNotes 2000-12
Microsoft ⁴³⁷	Internet Explorer 4.5, 5.0 for Macintosh	Windows 95/98/NT/ 2000, Mac OS	HTML Mail Attachment Vulnerability	Medium	CyberNotes 2000-01
Microsoft ⁴³⁸	Internet Explorer 4.x, 5.x	Windows 95/98/NT 4.0/2000	Internet Explorer Scriptlet Rendering	Medium	CyberNotes 2000-16
Microsoft ⁴³⁹	Internet Explorer 4.x, 5.x prior to version 5.5	Windows 95/98/NT 4.0/2000	IE Cached Web Credentials	Medium	CyberNotes-2000-21
Microsoft ⁴⁴⁰	Internet Explorer 5.4; Netscape Navigator 4.0; Outlook 2000, 98, Outlook Express 98; Eudora 4; Microsoft Word 97		Network File Resource	High	CyberNotes 2000-06
Microsoft ⁴⁴¹	Internet Explorer 5.0, 5.01	Windows 95/98/2000/NT	Microsoft Internet Explorer HTML Help Shortcut Vulnerability	High	CyberNotes 2000-05
Microsoft ⁴⁴²	Internet Explorer 5.0, 5.01; Outlook 97.0, 98, 2000; Outlook Express 5.0	Windows 95/98/NT 4.0/2000	Internet Explorer and Outlook/ Outlook Express Remote File Write	High	CyberNotes 2000-13
Microsoft ⁴⁴³	Internet Explorer 5.0.1	Windows 95/98/NT 3.5.1/4.0/2000	NavigateAndFind Vulnerability	High	CyberNotes 2000-01
Microsoft ⁴⁴⁴	Internet Explorer 5.01, 5.5	Windows 95/98/NT 4.0/2000	Internet Explorer Navigate Function Cross Frame Access	Medium	CyberNotes 2000-18
Microsoft ⁴⁴⁵	Internet Explorer 5.01, 5.5 (also affects Microsoft Outlook)	Windows 95/98/NT 4.0/2000	Internet Explorer DHTML & IFRAME File Read	Medium/High	CyberNotes 2000-15
Microsoft ⁴⁴⁶	Internet Explorer 5.01; Access 2000	Windows 95/98/NT 4.0/2000	Internet Explorer and Access 2000 VBA Code Execution	High	CyberNotes 2000-13
Microsoft ⁴⁴⁷	Internet Explorer 5.5	Windows 95/98/NT 4.0/2000	Internet Explorer Index.dat	High	CyberNotes-2000-24
Microsoft ⁴⁴⁸	Internet Explorer 5.x	Windows 95/98/2000 NT 4.0	Microsoft JScript Cross Frame Vulnerability	Medium	CyberNotes 2000-08
Microsoft ⁴⁴⁹	Internet Explorer 5.x	Windows 95/98/NT 4.0/2000	Internet Explorer Browser Print Template, File Upload via Form, & Scriptlet Rendering and Frame Domain Verification Vulnerabilities	Medium	CyberNotes-2000-25
Microsoft ⁴⁵⁰	Internet Information Server (IIS) 2.0, 3.0, 4.0, 5.0	Windows NT 4.0/2000	Internet Information Server IP Address Disclosure	Medium	CyberNotes 2000-15
Microsoft ⁴⁵¹	Internet Information Server (IIS) 4.0	Windows NT 4.0	Microsoft Chunked Transfer Encoding Buffer Overflow	Low	CyberNotes 2000-06
Microsoft ⁴⁵²	Internet Information Server (IIS) 4.0, 5.0	Windows NT 4.0/2000	Microsoft Myriad Escaped Characters	Low	CyberNotes 2000-08

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Microsoft ⁴⁵³	Internet Information Server (IIS) 4.0, 5.0	Windows NT 4.0	Undelimited .HTR Request and File Fragment Reading via .HTR	Medium	CyberNotes 2000-10
Microsoft ⁴⁵⁴	Internet Information Server (IIS) 4.0, 5.0	Windows NT 4.0/2000	Malformed Extension Data in URL	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-10
Microsoft ⁴⁵⁵	Internet Information Server (IIS) 4.0, 5.0	Windows NT 4.0/2000	Internet Information Server Directory Browser Argument	Medium	CyberNotes 2000-15
Microsoft ⁴⁵⁶	Internet Information Server (IIS) 4.0, 5.0	Windows NT 4.0/2000	Windows NT File Permission Canonicalization	Medium	CyberNotes 2000-16
Microsoft ⁴⁵⁷	Internet Information Server (IIS) 4.0, 5.0; FrontPage	Windows NT 4.0	IIS shtml.exe Path Disclosure	Medium	CyberNotes 2000-10
Microsoft ⁴⁵⁸	Internet Information Server (IIS) 5.0	Windows NT 2000	IIS Specialized Header	Medium	CyberNotes 2000-17
Microsoft ⁴⁵⁹	Internet Information Server (IIS) 5.0	Windows NT 2000	IIS 5.0 Indexed Directory Disclosure	Medium	CyberNotes 2000-20
Microsoft ⁴⁶⁰	Internet Information Server (IIS) 5.0 and prior		IIS Directory Structure IDQ/IDA Extension	Medium	CyberNotes 2000-02
Microsoft ⁴⁶¹	Internet Information Server 4.0	Windows NT 4.0	IIS ISAPI Buffer Overflow	High	CyberNotes-2000-23
Microsoft ⁴⁶²	Internet Information Server 4.0, 5.0	Windows NT 4.0/2000	IIS Web Server Folder Traversal	High	CyberNotes-2000-21
Microsoft ⁴⁶³	Internet Information Server 4.0, 5.0	Windows NT 4.0/2000	IIS Session ID Cookie Marking	Medium	CyberNotes-2000-22
Microsoft ⁴⁶⁴	Internet Information Server 4.0, Windows NT 4.0	Windows NT 4.0	Internet Information Server and Windows NT Invalid URL	Low	CyberNotes 2000-18
Microsoft ⁴⁶⁵	Internet Information Server 4.0; Site Server 3.0; Site Server Commerce Edition 3.0	Windows NT 4.0	Escape Character Parsing Vulnerability	High	CyberNotes 2000-01
Microsoft ⁴⁶⁶	Internet Information Server 4.0; Site Server 3.0; Site Server Commerce Edition 3.0	Windows NT 4.0	Virtual Directory Naming Vulnerability	High	CyberNotes 2000-01
Microsoft ⁴⁶⁷	Media Player 6.4, 7	Windows 95/98/NT 4.0/2000	Media Player .ASX Buffer Overrun & .WMS Script Execution Vulnerabilities	High	CyberNotes-2000-24
Microsoft ⁴⁶⁸	Microsoft Commercial Internet System 2.0, 2.5		Malformed IMAP Request Vulnerability	High	CyberNotes 2000-01
Microsoft ⁴⁶⁹	Microsoft Exchange Server 5.5	Windows NT 4.0	Malformed MIME Header	Low	CyberNotes-2000-22
Microsoft ⁴⁷⁰	Microsoft IIS Far East Edition 4.0, 5.0	Windows NT 4.0/2000	IIS Far East Edition DBCS File Disclosure	Medium	CyberNotes-2000-25
Microsoft ⁴⁷¹	Microsoft Office 2000	Windows 95/98/NT 4.0/2000	Microsoft Office 2000 DLL Execution	High	CyberNotes 2000-19
Microsoft ⁴⁷²	Microsoft Windows NT 2000	Windows NT 2000	Microsoft ActiveX Parameter Validation	Medium	CyberNotes-2000-22
Microsoft ⁴⁷³	Money 2000, 2001	Windows 95/98/NT 4.0/2000	Microsoft Money Password	Medium	CyberNotes 2000-17
Microsoft ⁴⁷⁴	NetMeeting Version 3.01 (4.4.3385)	Windows NT 4.0/2000	NetMeeting Desktop Sharing	Low	CyberNotes-2000-21
Microsoft ⁴⁷⁵	NT 4.0 Workstation, Server, Server Enterprise Edition, Terminal Server Edition, Windows 2000 Professional, Server, Advanced Server	Windows NT 4.0/2000	Windows NT Relative Shell Path	High	CyberNotes 2000-16
Microsoft ⁴⁷⁶	Outlook 5.x; Internet Explorer 5.x		Internet Explorer & Outlook Express .eml File	High	CyberNotes 2000-06
Microsoft ⁴⁷⁷	Outlook 97 8.02.4212	Windows 95/98/NT/ 2000	Microsoft Outlook 97 Denial of Service	Low	CyberNotes 2000-12

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Microsoft ⁴⁷⁸	Outlook 97, 98, 2000	Windows 95/98/NT 4.0	Outlook Winmail.dat	Medium	CyberNotes 2000-18
Microsoft ⁴⁷⁹	Outlook 97/98/2000; Windows Messaging, Exchange Client		Microsoft Mail Clients Denial of Service	Low	CyberNotes 2000-05
Microsoft ⁴⁸⁰	Outlook 98, 2000	Windows 95/98/NT 4.0	Outlook Vcard Denial of Service	Low	CyberNotes 2000-18
Microsoft ⁴⁸¹	Outlook 98, Outlook Express 4.x	Windows 98/98/NT 4.0	Outlook Long Filename	High	CyberNotes 2000-10
Microsoft ⁴⁸²	Outlook Express 4.0, 4.01, 5.0, 5.01	Windows 95/98/NT 4.0/2000	Outlook Express Persistent Mail-Browser Link	Medium	CyberNotes 2000-15
Microsoft ⁴⁸³	Outlook Express 4.0, 4.01, 5.0, 5.01, Outlook 97.0, 98, 2000	Windows 95/98/NT 4.0/2000	Outlook / Outlook Express Cache Bypass	Medium	CyberNotes 2000-15
Microsoft ⁴⁸⁴	Outlook Express 4.0, 4.01, 5.0, 5.01; Outlook 97.0, 98, 2000	Windows 95/98/NT 4.0	Outlook / Outlook Express Malformed E-mail Header	High	CyberNotes 2000-15
Microsoft ⁴⁸⁵	Outlook Express 4.27.3110.1, 4.72.2106.4, 4.72.3120.0, 4.72.3612.1700 Outlook Express 5.0; Outlook 98/2000; Internet Explorer 4x, 5x	Windows 95/98/NT 4.0/2000	Microsoft Signed ActiveX Active Setup	High	CyberNotes 2000-04
Microsoft ⁴⁸⁶	Outlook Express 5.0	Windows 95/98/NT 4.0	MS Outlook Express 5 JavaScript E-mail Access Vulnerability	Medium	CyberNotes 2000-03
Microsoft ⁴⁸⁷	Outlook Express 5.0, 5.01, 5.5; Internet Explorer 5.0 for Windows 95, 98, NT 4.0 & 2000, 5.01, 5.5	Windows 95/98/NT 4.0/2000	Internet Explorer / Outlook Express GetObject() File Disclosure	Medium	CyberNotes 2000-20
Microsoft ⁴⁸⁸	Site Server 3.0 Commerce Edition	Windows NT 4.0	MS Site Server Commerce Edition Input Validation	High	CyberNotes 2000-04
Microsoft ⁴⁸⁹	SQL Server 6.0, 6.5, 7.0	Windows NT 4.0	SQL Server Xp_sprintf buffer	High	CyberNotes 2000-10
Microsoft ⁴⁹⁰	SQL Server 7.0	Windows 95/98	Malformed TDS Packet Header Vulnerability	Low	CyberNotes 2000-01
Microsoft ⁴⁹¹	SQL Server 7.0	Windows NT 4.0	SQL Server Stored Procedure	Medium	CyberNotes 2000-14
Microsoft ⁴⁹²	SQL Server 7.0 Service Pack 1.0, 2.0, SQL Server 7.0	Windows NT 4.0	SQL Service Pack Password	Medium	CyberNotes 2000-11
Microsoft ⁴⁹³	SQL Server Version 7.0; Data Engine (MSDE) 1.0	Windows 95/98/NT 4.0/2000	SQL Query Abuse	High	CyberNotes 2000-05
Microsoft ⁴⁹⁴	Systems Management Server 2.0		Remote Agent Permissions	Medium	CyberNotes 2000-04
Microsoft ⁴⁹⁵	Visual Interdev 1.0	Windows 9x NT 4.0	Microsoft Link View Server-Side Component	High	CyberNotes 2000-08
Microsoft ⁴⁹⁶	Windows 2000	Windows 2000	Microsoft Windows 2000 Install Unprotected ADMIN\$ Share	Medium Note: This may be High risk in some installations	CyberNotes 2000-04
Microsoft ⁴⁹⁷	Windows 2000	Windows 2000	Windows 2000 Disk Quota Limitation	Low	CyberNotes 2000-05
Microsoft ⁴⁹⁸	Windows 2000	Windows 2000	Windows 2000 Still Image Service Privilege Escalation	High	CyberNotes 2000-18
Microsoft ⁴⁹⁹	Windows 2000 Advanced Server, Server, Professional	Windows NT 2000	Windows NT 2000 Local Security Policy Corruption	MediumHigh (High if DDoS best-practices not in place)	CyberNotes 2000-18
Microsoft ⁵⁰⁰	Windows 2000 Professional, Server, Advanced Server	Windows 2000	Windows 2000 Desktop Separation	Medium	CyberNotes 2000-12
Microsoft ⁵⁰¹	Windows 2000 Server & Professional	Windows NT 2000	Windows 2000 Default SYSKEY Configuration	Medium	CyberNotes 2000-10

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Microsoft ⁵⁰²	Windows 2000 Server; Advanced Server	Windows 2000	Mixed Object Access	Medium	CyberNotes 2000-08
Microsoft ⁵⁰³	Windows 95, 98	Windows 95/98	Windows 9x ARP Spoofing	Medium	CyberNotes 2000-13
Microsoft ⁵⁰⁴	Windows 95, 98, 98 SE, 98 ME, NT 4.0	Windows 95/98/98 SE/98 ME/NT 4.0	Windows Incomplete TCP/IP Packet	Low	CyberNotes-2000-24
Microsoft ⁵⁰⁵	Windows 95, 98, 98 Second Edition	Windows 95/98/98se	Windows Malformed IPX Ping Packet	Low	CyberNotes 2000-16
Microsoft ⁵⁰⁶	Windows 95, 98, 98 Second Edition; NT 4.0 Workstation 4.0 Server; Server Enterprise Edition; Server Terminal Server Edition	Windows 95/98/98se/NT 4.0	Malformed RTF Control Word	Low	CyberNotes 2000-02
Microsoft ⁵⁰⁷	Windows 95, 98, 98se	Windows 95/98/98se	Windows 9x Invalid Driver Type Denial of Service	Low	CyberNotes-2000-21
Microsoft ⁵⁰⁸	Windows 95, 98, 98se, ME	Windows 95/98/98se/ME	Windows 9x/ME Malformed IPX NMPI Packet	Low	CyberNotes-2000-21.
Microsoft ⁵⁰⁹	Windows 95, 98, 98se, ME	Windows 95/98/98se/ME	Windows 9x/ME Share Level Password	Medium	CyberNotes-2000-21
Microsoft ⁵¹⁰	Windows 95, 98, NT 4.0, NT 2000	Windows 95/98/NT 4.0/2000	Windows 9x / NT 4.0 / 2000 NetBIOS Cache Corruption	Medium/High (High if DDoS best-practices not in place)	CyberNotes 2000-18
Microsoft ⁵¹¹	Windows 95/98	Windows 95/98	Microsoft Windows 9x NetBIOS NULL Name	Low	CyberNotes 2000-09
Microsoft ⁵¹²	Windows 95/98 NT 4.0 Workstation, Server, Server Enterprise Edition, Server, Terminal Server Edition, 2000 Professional, Server, Advanced Server	Windows 95/98/NT 4.0/2000	IP Fragment Reassembly	Low	CyberNotes 2000-11
Microsoft ⁵¹³	Windows 95/98/ NT 4.0/2000, Windows NT Terminal Server	Windows 95/98/ NT 4.0/2000	ResetBrowser Frame and Host Announcement Flooding	Low	CyberNotes 2000-11
Microsoft ⁵¹⁴	Windows 95/98/NT	Windows 95/98/NT	Microsoft Windows Autorun.inf Privilege Escalation	Medium	CyberNotes 2000-04
Microsoft ⁵¹⁵	Windows 98, 98SE, ME, 2000 (Hilgraeve Hyper Terminal 6.0 and previous)	Windows 98/9se/ME/NT 4.0/2000	HyperTerminal Buffer Overflow	High	CyberNotes-2000-21
Microsoft ⁵¹⁶	Windows 98, 98SE, NT 2000	Windows 98/NT 2000	Windows 98/2000 Folder.htt	High	CyberNotes 2000-17
Microsoft ⁵¹⁷	Windows 98, Windows NT 4.0, 2000	Windows 98/NT 4.0/2000	Windows 98 / NT 4.0 / 2000 File Extension Validation	High	CyberNotes 2000-18
Microsoft ⁵¹⁸	Windows Media Encoder 4.0-4.1	Windows 95/98/NT	Malformed Windows Media Encoder Request	Low	CyberNotes 2000-11
Microsoft ⁵¹⁹	Windows Media License Manager 4.0, 4.1	Windows NT 4.0	Microsoft Malformed Media License Request	Low	CyberNotes 2000-06
Microsoft ⁵²⁰	Windows Media Player 7	Windows 95/98/NT 4.0/2000	Windows Media Player "OCX Attachment" Vulnerability	Low	CyberNotes 2000-20
Microsoft ⁵²¹	Windows Media Services 4.0, 4.1	Windows NT 4.0/2000	Microsoft Windows Media Services Handshake Sequence Denial of Service	Low	CyberNotes 2000-04
Microsoft ⁵²²	Windows Media Services 4.0, 4.1	Windows NT 4.0/2000	Windows Media Unicast Service Race Condition	Low	CyberNotes 2000-18
Microsoft ⁵²³	Windows NT	Windows NT	Microsoft Windows Shortcut	Low	CyberNotes 2000-03
Microsoft ⁵²⁴	Windows NT 2000	Windows NT 2000	Microsoft Windows 2000 Service Control Manager Named Pipe Impersonation	High	CyberNotes 2000-16
Microsoft ⁵²⁵	Windows NT 2000	Windows NT 2000	Windows 2000 Malformed RPC Packet	Low	CyberNotes 2000-19

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Microsoft ⁵²⁶	Windows NT 2000	Windows NT 2000	Windows 2000 Telnet Client NTLM Authentication	Medium	CyberNotes 2000-19
Microsoft ⁵²⁷	Windows NT 2000	Windows NT 2000	Windows NT 2000 Simplified Chinese IME State Recognition	High	CyberNotes 2000-20
Microsoft ⁵²⁸	Windows NT 2000	Windows NT 2000	Windows 2000 Telnet Session Timeout Denial of Service	Low	CyberNotes-2000-24
Microsoft ⁵²⁹	Windows NT 2000 Professional, Server, Advanced Server	Windows NT 2000	Windows 2000 Desktop Separation	Medium	CyberNotes 2000-13
Microsoft ⁵³⁰	Windows NT 2000 Professional, Server, Advanced Server, Datacenter	Windows NT 2000	Windows NT Domain Account Lockout	Medium	CyberNotes-2000-24
Microsoft ⁵³¹	Windows NT 2000, 2000.2072, 2000.2031, 2000.0.2195	Windows NT 2000	Windows 2000 Remote CPU-Overload	Low	CyberNotes 2000-14
Microsoft ⁵³²	Windows NT 3.5, 3.5.1, 4.0, 2000, Terminal Server; Microsoft Systems Management Server 1.2, 2.0	Windows NT 4.0	Microsoft Netmon Protocol Parsing	High	CyberNotes-2000-22
Microsoft ⁵³³	Windows NT 4.0	Windows NT 4.0	Microsoft Registry Permissions	High	CyberNotes 2000-05
Microsoft ⁵³⁴	Windows NT 4.0	Windows NT 4.0	NT Automated Tasks / Drive Mappings	High	CyberNotes 2000-06
Microsoft ⁵³⁵	Windows NT 4.0	Windows NT 4.0	Microsoft Windows NT 4.0 MSIEXEC Registry Permissions	Medium	CyberNotes-2000-22
Microsoft ⁵³⁶	Windows NT 4.0	Windows NT 4.0	Windows NT SynAttack Protect Denial of Service	Low	CyberNotes-2000-24
Microsoft ⁵³⁷	Windows NT 4.0 Server, Enterprise Edition, Windows 2000 Server, Advanced Server	Windows NT 4.0/2000	Windows NT Phone Book Service Buffer Overflow	High	CyberNotes-2000-25
Microsoft ⁵³⁸	Windows NT 4.0 Terminal Server Edition	Windows NT 4.0	Registry Enumeration File	Low	CyberNotes 2000-02
Microsoft ⁵³⁹	Windows NT 4.0 Workstation; 4.0 Server; 4.0 Server Enterprise Edition; 4.0 Server Terminal Server Edition	Windows NT 4.0	Spoofed LPC Port Request	High	CyberNotes 2000-02
Microsoft ⁵⁴⁰	Windows NT 4.0 Workstation, Server, Enterprise Edition, Terminal Server Edition; Windows 2000 Professional, Server, Advanced Server, Datacenter Server	Windows NT 4.0/2000	Microsoft Multiple LPC and LPC Ports Vulnerabilities	Medium	CyberNotes 2000-20
Microsoft ⁵⁴¹	Windows NT 4.0 Workstation, Server, Enterprise Server Edition, Terminal Server Edition	Windows NT	Windows NT Remote Registry Access Authentication	Low	CyberNotes 2000-12
Microsoft ⁵⁴²	Windows NT 4.0 Workstation, Server, Enterprise Edition, Terminal Server Edition, Windows 2000	Windows NT 4.0/2000	Windows NT NetBIOS Name Server Protocol Spoofing	Medium	CyberNotes 2000-15
Microsoft ⁵⁴³	Windows NT 4.0, 2000	Windows NT 4.0/2000	Windows NT Unspecified Executable Path	High	CyberNotes 2000-15.
Microsoft ⁵⁴⁴	Windows NT 4.0, 2000; Windows NT Terminal Server	Windows NT 4.0/2000	TCP/IP Printing Service Denial of Service	Low	CyberNotes 2000-07
Microsoft ⁵⁴⁵	Windows NT Server 4.0 with Internet Information Server 4.0	Windows NT	InetInfo.Exe Denial of Service	Low	CyberNotes 2000-04
Microsoft ⁵⁴⁶	Windows NT Terminal Server	Windows NT	Windows NT Terminal Server Login Buffer Overflow	High	CyberNotes-2000-23

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Microsoft ⁵⁴⁷	Windows NT Terminal Server, NT 4.0	Windows NT 4.0	Microsoft NT Offload ModExpo Registry Permissions	Medium	CyberNotes 2000-08
Microsoft ⁵⁴⁸	Windows NT Workstation 4.0; Server 4.0; Server 4.0, Enterprise Edition	Windows NT 4.0	Microsoft Recycle Bin Creation	Medium	CyberNotes 2000-03
Microsoft ⁵⁴⁹	Word 97, 2000	Windows 95/98/NT 4.0/2000	Word Mail Merge	High	CyberNotes 2000-20
Microsoft ⁵⁵⁰	Wordpad		Wordpad Embedded Command	High	CyberNotes 2000-05
Microsoft ^{551, 552}	Internet Information Services 4.0, 5.0	Windows NT 4.0/2000	IIS Web Server File Request Parsing	High	CyberNotes-2000-23, CyberNotes-2000-24.
Microsoft ^{553, 554}	Microsoft Outlook 97.0, 98, 2000; Internet Explorer 4.0 for Windows 3.1, 95, 98, NT 3.51, NT 4.0; Internet Explorer 5.0 for Windows 95, 98, NT 4.0, 2000, 5.01, 5.5	Windows 95/98/NT 4.0/2000	Internet Explorer / Outlook Express Com.ms.activeX.Active Xcomponent Arbitrary Program Execution	High	CyberNotes 2000-20, CyberNotes-2000-21
Microsoft ^{555, 556}	Microsoft VM (all builds in the 2000 series, 3100-3300 series)	Windows 95/98/NT 4.0/2000	Microsoft VM ActiveX Component	Medium	CyberNotes 2000-17, CyberNotes-2000-21
Microsoft ^{557, 558}	WebTV for Windows	Windows ME/98/98SE	Microsoft WebTV Denial of Service	Low	CyberNotes 2000-19, CyberNotes-2000-21
Microsoft ^{559, 560}	Windows 95/98	Windows 95/98	Windows 95/98 Device Driver Denial of Service	Low	CyberNotes 2000-05, CyberNotes 2000-06
Microsoft ^{561, 562}	Windows NT 4.0, 4.0 Server, Enterprise Edition, Terminal Server Edition; Windows 2000 Professional, 2000 Server, 2000 Advanced Server	Windows NT 4.0/2000	Windows NT Registry Permissions	Medium	CyberNotes-2000-25
Microsoft ^{563, 564}	Internet Information Server (IIS) 4.0, 5.0; FrontPage 2000 Server Extensions 1.2	Windows 95/98/ NT 4.0/2000	FrontPage/IIS Cross-Site Scripting	Medium	CyberNotes 2000-17, CyberNotes-2000-22
Microsoft ^{565, 566}	Excel 97, 2000	Windows 95/98/NT 4.0/2000	Excel 97/2000 Register.ID	High	CyberNotes 2000-14, CyberNotes 2000-15
Microsoft ^{567, 568}	Internet Explorer 4/5 All builds in the 2000, 3100, and 3200 Series	Windows 95/98/NT 4.0/2000	Microsoft Java Virtual Machine GetSystemResourceAs Stream	Very High	CyberNotes 2000-03, CyberNotes 2000-04
Microsoft ^{569, 570}	Microsoft SQL Server 7.0; Enterprise Manager Server	Windows NT/2000	SQL Server DTS Password	Medium	CyberNotes 2000-12, CyberNotes 2000-14
Microsoft ^{571, 572}	Windows NT 2000	Windows NT 2000	Microsoft Windows 2000 Protected Store Key Length	High	CyberNotes 2000-11, CyberNotes 2000-15
Microsoft ^{573, 574}	Windows NT 2000, 2000.2072, 2000.2031, 2000.0.2195	Windows NT 2000	Windows 2000 Telnet Server Denial of Service	Low	CyberNotes 2000-14, CyberNotes 2000-15
Microsoft ^{575, 576, 577}	PowerPoint 2000; Internet Explorer 5.01	Windows 95/98/NT 4.0/2000	Internet Explorer and Excel/ PowerPoint 2000 ActiveX Object Execution or Office HTML Script and IE Script Vulnerabilities	High	CyberNotes 2000-13, CyberNotes 2000-14, CyberNotes 2000-16
Microsoft ^{578, 579}	Index Server 2.0; Windows 2000 Indexing Service	Windows NT 4.0	Malformed Hit-Highlighting Argument	Medium/Low	CyberNotes 2000-02, CyberNotes 2000-03
Microsoft ^{580, 581}	Microsoft Outlook Express 4.0, 5.0, 5.01, 5.5; Outlook 97, 98, 2000; Internet Explorer 4.0.1, 4.1, 5.0, 5.01, 5.5	Windows 95/98/NT 4.0/2000	Microsoft VM File Reading	Medium	CyberNotes-2000-21, CyberNotes-2000-22
Microsoft/ Apple ⁵⁸²	MacOS Runtime for Java (MRJ) version 2.1 and 2.0 with Internet Explorer	Mac OS	Macintosh MRJ Java Security Hole in URL Connection	Medium	CyberNotes 2000-12.

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Microsys ⁵⁸³	CyberPatrol 4.04.003, 4.04.005		CyberPatrol Insecure Registration	Medium	CyberNotes-2000-24
Midnight Commander ⁵⁸⁴	Midnight Commander 4.5.40-4.5.51	Unix	Midnight Commander Directory Viewing Command Execution	High	CyberNotes-2000-24
Midstream ⁵⁸⁵ (Original report in German)	PrivateExE		PrivateExE dll password override	Low	CyberNotes 2000-01
MIT ⁵⁸⁶	Kerberos 4 4.0 patch 10, Kerberos 5 5.0-1.2beta1, 5.0-1.2beta2, 5.0-1.1.1		Kerberos KDC Spoofing	Low	CyberNotes 2000-18
MIT ⁵⁸⁷	MIT Kerberos 5 releases krb5-1.0.x, krb5-1.1.1, MIT Kerberos 4 patch 10 and below, KerbNet, Cygnus Network Security, & KTH-krb4 below version .10		Kerberos KRB4 KDC	High	CyberNotes 2000-12
Mobius ⁵⁸⁸	Document Direct for the Internet 1.2	Windows NT 4.0	Document Direct Buffer Overflow	High	CyberNotes 2000-19
Multiple Firewall Vendors ⁵⁸⁹	Checkpoint Software Firewall-1 3.0, 4.0; Cisco PIX Firewall 4.1.6, 4.1.6b, 4.2.1, 4.2.2, 4.3, 4.4(4), 5.0, 5.1		Multiple Firewall Vendor FTP "ALG" Client	High	CyberNotes 2000-06
Multiple Firewalls ^{590, 591}	Multiple Firewalls		Multiple Firewall FTP Application Level Gateway PASV	High	CyberNotes 2000-03, CyberNotes 2000-06
Multiple Linux Vendors ⁵⁹²	Alessandro Rubini gpm 1.19, 1.18.1; Debian Linux 2.2pre potato, 2.0-2.2; RedHat 6.0 i386, 6.1 i386	Unix	Multiple Linux Vendor gpm Setgid	High	CyberNotes 2000-06
Multiple Linux Vendors ⁵⁹³	Halloween Linux 4.0	Unix	Imwheel Root Compromise	High	CyberNotes 2000-06
Multiple Linux Vendors ⁵⁹⁴	Halloween Linux 4.0; SuSE Linux 6.0-6.3	Unix	Multiple Linux Vendor kreatecd	High	CyberNotes 2000-06
Multiple Linux Vendors ^{595, 596, 597}	Michael Sandrof IrcII 4.4-7 for SuSE Linux 6.3; RedHat Linux 6.1 i386	Unix	IrcII DCC Chat Buffer Overflow	High	CyberNotes 2000-06, CyberNotes 2000-07, CyberNotes 2000-08
Multiple Vendors ⁵⁹⁸	Allaire JRun 2.3.x	Unix	Allaire JRun 2.3.x Sample Files	Low	CyberNotes 2000-13
Multiple Vendors ⁵⁹⁹	APC Apcupsd 3.7.2	Unix	APC Apcupsd Local Denial of Service	Low	CyberNotes-2000-25
Multiple Vendors ⁶⁰⁰	BB4 Big Brother Network Monitor 1.5d2 and previous	Unix	BB4 Big Brother Multiple CGI Vulnerabilities	Medium	CyberNotes-2000-24
Multiple Vendors ⁶⁰¹	BeOS r4.5, r4.5-2, r5 pro; Felix-2-3-R4 (IRC Client); Baxter (IRC Client); Bowser (IRC Client); PostMaster-1.0 (E-mail Client); RobinHood-1.1 (HTTPD)	BeOS	Multiple Vendor BeOS Buffer Overflow	High	CyberNotes-2000-23
Multiple Vendors ⁶⁰²	BitchX IRC Client 1.0c16, 75.0p1, 75.0p3	Unix	BitchX IRC Client Denial of Service	High	CyberNotes 2000-14
Multiple Vendors ⁶⁰³	Caldera eDesktop 2.4, eServer 2.3, OpenLinux Desktop 2.3; HP HP-UX 11.11; MandrakeSoft Linux Mandrake 6.0, 6.1, 7.0-7.2; RedHat Linux 5.2, 6.0-6.2E sparc, i386, alpha; SuSE Linux 7.0; Sun Solaris 8.0; Wirex Immunix OS 6.2	Unix	Multiple Vendor Bash/temp File Symlink	High	CyberNotes-2000-24

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ⁶⁰⁴	Caldera eServer 2.3, OpenLinux Desktop 2.3, eBuilder 3.0; Conectiva Linux 4.0-5.2; Linux 2.0-2.3; MandrakeSoft Linux Mandrake 7.0, 7.1; RedHat Linux 5.1-6.2; SuSE Linux 6.1-7.0; SGI 6.2-6.5.8; Slackware Linux 7.0, 7.1; Sun Solaris 2.0-2.6, 7.0, 8.0; Trustix Secure Linux 1.0, 1.1	Unix	Multiple Vendor Locale Subsystem Format String	High	CyberNotes 2000-18
Multiple Vendors ⁶⁰⁵	Caldera OpenLinux 2.2-2.4; Conectiva Linux 3.0, 4.0, 4.0es, 4.1, 4.2, 5.0; Debian GNU/Linux 2.1-2.3; Red Hat Linux 6.1, 6.2; Slackware Linux 7.0, 7.1; Washington University wu-ftpd 2.4.2, 2.5, 2.6	Unix	Wu-Ftpd Remote Format String Stack Overwrite	High	CyberNotes 2000-13
Multiple Vendors ⁶⁰⁶	Caldera OpenLinux 2.4; Debian Linux 2.2, 2.3; RedHat Linux 6.2 & 6.2E alpha, i386, sparc, 7.0; SGI IRIX 5.2, 5.3, 6.3; Sun Solaris 2.6_x86HW3/98, 2.6_x86, 2.6, 2.5.1_x86, 2.5.1_ppc, 2.5.1, 2.5_x86, 2.5, 2.4_x86	Unix	Multiple Vendor Mail 'Reply-To' Field	Medium/High	CyberNotes-2000-23
Multiple Vendors ⁶⁰⁷	Colten Edwards BitchX 1.0c17	Unix	BitchX Multiple Vulnerabilities	High	CyberNotes-2000-25
Multiple Vendors ⁶⁰⁸	Debian Linux 2.1, 2.2; FreeBSD 1.1.5.1, 2.0, 2.0.5, 2.1, 2.1.5, 2.1.6, 2.1.1.6, 2.1.7.1; NetBSD 1.0-1.4.2 ; OpenBSD 2.0-2.7; ProFTPD 1.2pre1-1.2pre9; 1.3	Unix	Multiple Vendor FTPD Input Validation	High	CyberNotes 2000-14
Multiple Vendors ⁶⁰⁹	Eric Rescorla ssldump 0.9b1 and previous	Unix	ssldump Format String	High	CyberNotes-2000-25
Multiple Vendors ⁶¹⁰	FreeBSD 3.2-3.5, 4.0; NetBSD 1.4-1.4.2; OpenBSD 2.3-2.7	Unix	Multiple Vendor BSD Libutil Pw_error() Format String	High	CyberNotes 2000-20
Multiple Vendors ⁶¹¹	Gerald Combs Ethereal 0.8.13 and previous	Unix	Ethereal AFS Buffer Overflow Vulnerabilities	High	CyberNotes-2000-24
Multiple Vendors ⁶¹²	Gert Doering Mgetty 1.1.19-1.1.21	Unix	Multiple Vendor Mgetty Symbolic Link Traversal	High	CyberNotes 2000-18
Multiple Vendors ⁶¹³	GNU Emacs 20.0-20.6	Unix	GNU EMACS 20 Vulnerabilities	Medium/High (High in multi-user environments)	CyberNotes 2000-08
Multiple Vendors ⁶¹⁴	Gossamer Threads DBMan 2.0.4	Windows 95/98, Unix	Gossamer Threads DBMan Information Leakage	Medium	CyberNotes 2000-10
Multiple Vendors ⁶¹⁵	Helsinki University of Technology SSH 1.2.14-1.2.27; OpenSSH 1.2, 1.2.3	Unix	SSH File Create/Overwrite	Medium	CyberNotes 2000-20
Multiple Vendors ⁶¹⁶	id Software Quake 1.9; J. P. Grossman ProQuake 1.0		Quake Server Empty UDP Denial of Service	Low	CyberNotes-2000-23
Multiple Vendors ⁶¹⁷	Igor Khasilev Oops Proxy Server 1.4.22 and previous	Unix	Multiple Vendor Oops Proxy Server Buffer Overflow	High	CyberNotes-2000-25
Multiple Vendors ⁶¹⁸	ISC BIND 8.2-8.2.2-P6	Windows, Unix	Multiple Vendor BIND Denial of Service	Low	CyberNotes-2000-23

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ⁶¹⁹	Jan Hubicka Koules 1.4	Unix	Koules Svalglib Buffer Overflow	High	CyberNotes-2000-24
Multiple Vendors ⁶²⁰	Jason Hines phpWebLog 0.4.2	Unix	phpWebLog Administrator Authentication Bypass	High	CyberNotes-2000-25.
Multiple Vendors ⁶²¹	John Donoghue Knapster 0.9; Josh Guilfoyle Gnapster 1.3.8	Unix	Gnapster & Knapster File Access	Medium	CyberNotes 2000-10
Multiple Vendors ⁶²²	Joseph Engo phpGroupWare 0.9.6 and prior	Unix	phpGroupWare Remote Include File	High	CyberNotes-2000-25
Multiple Vendors ⁶²³	KDE 1.1, 1.1.1, 1.1.2, 1.2, 2.0 BETA; Open Group X 11.0R6, 11.0R6.1, 11.0R6.2, 11.0R6.3; Wings wdm 1.2; XFree86 X11R6 3.3.3-3.3.6, 4.0	Unix	xdm/kdm/wdm Buffer Overflow	Low	CyberNotes 2000-13
Multiple Vendors ⁶²⁴	kon2-0.3.9	Unix	KON2 Buffer Overflow	High	CyberNotes 2000-13
Multiple Vendors ⁶²⁵	LCDProc 0.4	Unix	Multiple Vendor Linux LCDProc Buffer Overflow	High	CyberNotes 2000-09
Multiple Vendors ⁶²⁶	Leif M. Wright ad.cgi 1.0	BeOS, Unix	Leif M. Wright ad.cgi Unchecked Input	High	CyberNotes-2000-25
Multiple Vendors ⁶²⁷	Lexmark MarkVision 4.3 and previous	Unix	Lexmark MarkVision Printer Driver Buffer Overflow	High	CyberNotes-2000-25
Multiple Vendors ⁶²⁸	Linux 2.1, 2.2, 2.2pre potato Linux kernel 2.2.10, 2.2.12, 2.2.14; Linux 6.0, 6.1, 6.2	Unix	Linux Kernel IP Masquerading	High	CyberNotes 2000-07
Multiple Vendors ⁶²⁹	Linux 2.2.12, 2.2.14, 2.3.99-pre2	Unix	Linux Domain Socket Denial of Service	Low	CyberNotes 2000-07
Multiple Vendors ⁶³⁰	Linux 2.3, Linux 2.4.0-test1, & Linux 2.1.15 and below	Unix	Linux Capabilities Root Compromise	High	CyberNotes 2000-12
Multiple Vendors ⁶³¹	Linux kernel 2.2.10, 2.2.12-2.2.17	Unix	Linux Non-Readable File Ptrace	Medium	CyberNotes-2000-25
Multiple Vendors ⁶³²	L-Soft Listserv 1.8	Windows 95/98/NT 4.0, Unix	L-Soft Web Archives Buffer Overflow	High	CyberNotes 2000-09
Multiple Vendors ⁶³³	Luca Deri ntop 1.1pre3, 1.2a10, 1.2a7-9, 1.3.1, 1.3.2	Unix	Multiple Vendor Ntop-i Local Format String	High	CyberNotes-2000-22
Multiple Vendors ⁶³⁴	Max-Wilhelm Bruker bftpd 1.0.11	Unix	bftpd Buffer Overflow	Low	CyberNotes-2000-22
Multiple Vendors ⁶³⁵	Multiple Vendors (3COM, Cray, HP, Sun/Sparc, Windows, etc.)	Windows, Unix	Multiple Vendor SNMP World Writable Community	High	CyberNotes 2000-04
Multiple Vendors ⁶³⁶	NetBSD 1.4-1.4.2; OpenBSD 2.3-2.7	Unix	Multiple Vendor BSD eeprom Format String	High	CyberNotes 2000-20
Multiple Vendors ⁶³⁷	Netscape Communicator 4.0, 4.5, 4.51, 4.6, 4.61, 4.7, 4.72; Microsoft Internet Explorer 5.01, 5.5	Windows 95/98/NT 4.0/2000, Unix	Multiple Vendor 'Type=password' Denial of Service	Low	CyberNotes 2000-20
Multiple Vendors ⁶³⁸	Open Group X 11.0R6.1, 6.2, 6.3, 6.4; XFree86 X11R6 3.3.3, 3.3.4, 3.3.5, 3.3.6, 4.0; RedHat Linux 6.1, 6.2	Unix	XDMCP Infinite Loop Denial of Service	High	CyberNotes 2000-13
Multiple Vendors ⁶³⁹	OpenBSD 2.3-2.7; RedHat Linux 5.0, 5.1, 5.2 alpha, i386, sparc	Unix	BSD Talked Remote Format String	High	CyberNotes-2000-21
Multiple Vendors ⁶⁴⁰	PHP 3.00, 4.00	Unix	PHP Error Logging Format String	Medium	CyberNotes-2000-21
Multiple Vendors ⁶⁴¹	Qualcomm qpopper 3.0, 2.53; RedHat imap 4.5-4; University of Washington imap 4.5	Unix	Closed Mail Server	High	CyberNotes 2000-09
Multiple Vendors ⁶⁴²	RedHat Linux 6.x; XFree86 3.3.5-3.3.6, 4.0.0	Unix	Multiple Vendor X Font Server Denial of Service & Buffer Overflow	High	CyberNotes 2000-08
Multiple Vendors ⁶⁴³	SCO UnixWare 7.1.0 (Intel) Double Vision (from Tridia Corp) version 3.07.00	Unix	DoubleVision Local Root	High	CyberNotes 2000-19

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ⁶⁴⁴	Sun - Netscape Alliance iPlanet Certificate, Management System 4.2 for Windows NT 4.0, Netscape Directory Server 4.12	Windows NT 4.0	iPlanet CMS/Netscape Directory Server Plaintext Administrative Password And Directory Traversal	Medium	CyberNotes-2000-22
Multiple Vendors ⁶⁴⁵	Sun StarOffice 5.2	Unix	StarOffice /tmp Directory Symbolic Link	High	CyberNotes-2000-23
Multiple Vendors ⁶⁴⁶	SuSE Linux 4.0-4.4.1, 5.0- 5.3, 6.0-6.4, 7.0; Slackware Linux 3.3, 3.4, 3.5, 3.6, 3.9, OpenLinux 7.0; TurboLinux Turbo Linux 6.0-6.0.2	Unix	Multiple Linux Vendor fdmount Buffer Overflow	High	CyberNotes 2000-11
Multiple Vendors ⁶⁴⁷	SuSE Linux 6.4, RedHat Linux 6.1 (using the program cda); FreeBSD, OpenBSD (using the program /usr/bin/systat); Caldera Linux	Unix	Ncurses Buffer Overflows	Medium	CyberNotes-2000-21
Multiple Vendors ⁶⁴⁸	SuSE. Linux 6.4,7.0; RedHat Linux 7.0; Immunix OS 6.2, 7.0-beta; Linux-Mandrake 7.1, 7.2 (GNU Linux modutils 2.3.9)	Unix	Linux Modprobe Arbitrary Command Execution	High	CyberNotes-2000-23
Multiple Vendors ⁶⁴⁹	Wirex Immunix OS 6.2, 7.0- Beta; SuSE Linux 6.4, 7.0; RedHat Linux 7.0; MandrakeSoft Linux Mandrake 7.2; Conectiva Linux 5.1; (GNU Linux modutils 2.3.11, 2.3.9)	Unix	Multiple Vendor Linux modprobe Buffer Overflow	High	CyberNotes-2000-24
Multiple Vendors ⁶⁵⁰	Wmcdplay		Wmcdplay Local Root Compromise	High	CyberNotes 2000-06
Multiple Vendors ⁶⁵¹	XChat 1.3.10-1.3.13, 1.3.9, 1.4, 1.4.1-1.4.2, 1.5.x dev	Unix	X-Chat Command Execution Via URLs	High	CyberNotes 2000-17
Multiple Vendors ⁶⁵²	XFree86 X11R6 3.3.3-3.3.6, 4.0; Open Group X 11.0R5, 6, 6.1-6.4; GNOME 1.0.x, 1.1	Unix	LibICE Denial of Service	Low/High (High if DDos best-practices not in place)	CyberNotes 2000-13
Multiple Vendors ⁶⁵³	Xlockmore 4.16 and below	Unix	Multiple Vendor Xlockmore Memory Reading Vulnerability	High	CyberNotes 2000-11
Multiple Vendors ⁶⁵⁴ , 655, 656, 657	Zope 1.10.3, 2.1.x, 2.1.1, 2.1.7, 2.2 beta1	Unix	Zope Unauthorized Role Modification	Medium	CyberNotes 2000-17
Multiple Vendors 658, 659, 660	Caldera OpenLinux 2.3, 2.4; Mandrake 6.0, 6.1, 7.0, 7.1; RedHat Linux 5.2, 6.0, 6.1. 6.2 alpha, i386, sparc	Unix	Multiple Vendor man(1) 'makewhatis' Insecure /tmp Files	Medium	CyberNotes 2000-14
Multiple Vendors ⁶⁶¹ , 662	Conectiva Linux 4.0-4.2, 5.0-5.1; RedHat Linux 6.0- 6.2 alpha, i386, sparc	Unix	Multiple Linux Vendor pam Remote User	Medium	CyberNotes 2000-15
Multiple Vendors ⁶⁶³ , 664	David Bagley xlock 4.16, 4.16.1	Unix	Xlockmore User Supplied Format String	Medium	CyberNotes 2000-17
Multiple Vendors ⁶⁶⁵ , 666	Debian Linux 2.1, 2.2pre potato; FreeBSD 3.5, 4.0, 5.0 alpha,	Unix	Canna Remote Buffer Overflow	High	CyberNotes 2000-14
Multiple Vendors ⁶⁶⁷ , 668	FreeBSD wu-ftp port, versions 2.6.0 and below; NetBSD wu-ftp versions prior to 2.6.1	Unix	Multiple Vendor Wu-ftp	High	CyberNotes 2000-14

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ^{669, 670}	FreeBSD 5.0, 5.0 alpha, FreeBSD 4.0, 4.0 alpha, FreeBSD 3.x, 2.2.8, 2.2.2-2.2.6, 2.2, 2.1.7.1, 2.1.6.1, 2.1.6, 2.1.5, 2.1, 2.0.5, 2.0, 1.1.5.1; All NetBSD prior to 2000/05/27; OpenBSD 2.6, 2.5, 2.4, 2.3, 2.2, 2.1, 2.0	Unix	Multiple Vendor BSD Semaphore IPC Denial Of Service	Low	CyberNotes 2000-11
Multiple Vendors ^{671, 672}	GNU Mailman 2.0beta3, 2.0beta4	Unix	GNU Mailman Local Format String Stack Overwrite	Medium	CyberNotes 2000-16
Multiple Vendors ^{673, 674}	Lawrence Berkeley National Laboratory's traceroute 1.4a5; Debian potato; RedHat 6.0, 6.2; Caldera 2.4; Mandrake 7.0; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1; Solaris 2.5.1	Unix	Multiple Vendor Traceroute Heap Corruption	High	CyberNotes 2000-20, CyberNotes-2000-21
Multiple Vendors ^{675, 676}	Luca Deri ntop 1.2a7-9	Unix	Linux Ntop Unauthorized File Retrieval	High	CyberNotes 2000-16
Multiple Vendors ^{677, 678}	NetBSD 1.4.1 & 1.4.2 x86, arm32, SPARC, Alpha; OpenBSD 2.4-2.7; RedHat Powertools 6.0-6.2	Unix	Multiple Vendor Mopd Buffer Overflow	High	CyberNotes 2000-16
Multiple Vendors ^{679, 680}	RedHat Linux 6.1, 6.2; Mandrake 7.0	Unix	RedHat Openldap Symlink Overwrite Denial	Medium	CyberNotes 2000-09
Multiple Vendors ^{681, 682}	Turbo Linux 3.5b2, 4.2, 4.4, 6.02; Matt Kimball and Roger Wolff mtr 0.28, 0.41	Unix	Multiple Vendor mtr	High	CyberNotes 2000-05
Multiple Vendors ^{683, 684}	4.0, 4.0es, 4.1, 4.2, 5.0	Unix	Restore Buffer Overflow	High	CyberNotes 2000-14
Multiple Vendors ^{685, 686, 687}	Caldera eDesktop 2.4, eServer 2.3; OpenLinux Desktop 2.3, eBuilder 3.0; RedHat Linux 7.0; NetBSD 1.4-1.4.2; OpenBSD 2.7; Immunix OS 6.2	Unix	Multiple Vendor LPRng User-Supplied Format String	High	CyberNotes 2000-20
Multiple Vendors ^{688, 689, 690}	Conectiva Linux 4.0-4.2, 5.0-5.1; OpenLinux eDesktop 2.4, OpenLinux eServer 2.3 and OpenLinux eBuilder, OpenLinux Desktop 2.3; Red Hat Linux 5.2 and 6.x	Unix	Linux GPM File Removal	Medium	CyberNotes 2000-15
Multiple Vendors ^{691, 692, 693}	GNOME GnoRPM 0.94 and earlier; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1; RedHat Linux 6.1, 6.2, and 7.0	Unix	GnoRPM Arbitrary File Overwrite	High	CyberNotes 2000-20, CyberNotes-2000-23
Multiple Vendors ^{694, 695, 696}	Joseph Allen Joe 2.8	Unix	Joe Text Editor Symbolic Link	Medium	CyberNotes-2000-24
Multiple Vendors ^{697, 698, 699}	Larry Wall Perl 5.004_05, 5.005_003, 5.6	Unix	SuidPerl Mail Shell Escape	High	CyberNotes 2000-16
Multiple Vendors ^{700, 701, 702, 703, 704}	RedHat Linux 6.2 alpha, i386, sparc, 7.0; Immunix OS 6.2; Mandrake 6.0, 6.1, 7.0, 7.1; Trustix Secure Linux (all versions); Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1	Unix	Tmpwatch Arbitrary Command Execution	High	CyberNotes-2000-21
Multiple Vendors ^{705, 706}	Conectiva Linux 4.0-4.2, 5.0; Debian Linux 2.2, 2.3; RedHat Linux 6.0-6.3; Trustix Secure Linux 1.0, 1.1	Unix	Multiple Vendor Rpc.statd Remote Format String Stack Overwrite	High	CyberNotes 2000-15, CyberNotes 2000-16

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Multiple Vendors ^{707, 708}	Cygnus Network Security 4.0.x, KerbNet 5.0.x; MIT Kerberos 4 4.0 patch 10, 5 5.0-1.1.1, 5 5.0-1.0.x		Kerberos Compatibility krb_rd_req() Buffer Overflow	High	CyberNotes 2000-10, CyberNotes 2000-11
Multiple Vendors ^{709, 710}	Juergen Weigert screen 3.9.3-3.9.5	Unix	Screen User Supplied Format String	High	CyberNotes 2000-18, CyberNotes 2000-19
Multiple Vendors ^{711, 712}	Majordomo 1.94.5		Majordomo Insecure Implementation Vulnerability	High	CyberNotes 2000-11, CyberNotes 2000-12
Multiple Vendors ^{713, 714, 715, 716}	Debian Linux 2.1, 2.2; ISC DHCP Client 2.0, 3.0b1; NetBSD-1.4.2 and prior; SuSE 6.1-6.4; Mandrake 6.0, 6.1, 7.0, 7.1	Unix	ISC DHCP Client Remote Root	High	CyberNotes 2000-13, CyberNotes 2000-14
Multiple Vendors ^{717, 718, 719, 720}	Samba pam_smb 0.23, 1.1.5	Unix	Samba PAM Modules Buffer Overflow	High	CyberNotes 2000-19
Multiple Vendors ^{721, 722, 723, 724, 725, 726, 727, 728}	Conectiva Linux 4.0-4.2, 5.0-5.1; Corel Linux OS 1.0; Debian Linux 2.2pre potato, 2.2, 2.3 (sparc, powerpc, arm, alpha); Immunix OS 6.2; MandrakeSoft Linux 6.0-6.1, 7.0-7.1; RedHat Linux 5.2, 6.0, 6.1, 6.2 (sparc, i386, alpha), 6.2E alpha; SuSE. Linux 6.2, 6.3 (alpha, ppc), 6.4 (alpha, ppc), 7.0 sparc; Slackware Linux 4.0, 7.0-7.1, Trustix Secure Linux 1.0, 1.1; TurboLinux 4.4, 6.0-6.0.4	Unix	Multiple Vendor Linux klogd Vulnerabilities	High	CyberNotes 2000-19
Multiple Web Shopping Carts ⁷²⁹	Web Shopping Carts		Web Shopping Carts HTTP Referer Headers	High	CyberNotes 2000-03
Multisoft ⁷³⁰	FlagShip 4.4	Unix	FlagShip Installation Permission	High	CyberNotes 2000-17
Nathan Purciful ⁷³¹	phpPhotoAlbum 0.9.9	Windows NT 4.0/2000, Unix	PhpPhoto Album Directory Traversal	Medium	CyberNotes 2000-18
NBase-Xyplex ⁷³²	EdgeBlaster MultiFunction WAN Access Router		EdgeBlaster Denial of Service	Low	CyberNotes 2000-07
NetBSD ⁷³³	NetBSD 1.4.1 and prior; NetBSD-current until 20000126	Unix	NetBSD Profs Security	High	CyberNotes 2000-04
NetBSD ⁷³⁴	NetBSD 1.4.2 Ftpchroot	Unix	NetBSD ftpchroot Vulnerability	Medium/High	CyberNotes 2000-11
NetBSD ⁷³⁵	NetBSD/vax 1.4.1 and earlier; -current prior to 19991212	Unix	Ptrace(2)'d Hardware Privileges	Medium	CyberNotes 2000-04
NetBSD ⁷³⁶	Shigio Yamaguchi Global 3.55	Unix	NetBSD Global Port Package CGI	High	CyberNotes-2000-22
NetBSD ^{737, 738}	NetBSD 1.4.2 SPARC, Alpha; 1.4.1 SPARC, Alpha; 1.4 SPARC, Alpha	Unix	NetBSD Unaligned IP Option Denial of Service	Medium/High (High if DDoS best-practices not in place)	CyberNotes 2000-09, CyberNotes 2000-10
NetcPlus ⁷³⁹	BrowseGate 2.80	Windows NT 4.0/2000	BrowseGate Denial of Service	Low	CyberNotes 2000-19
NetcPlus ⁷⁴⁰	BrowseGate 2.80.2	Windows 95/98/NT 4.0/2000	BrowseGate Weak Encryption	Medium	CyberNotes-2000-24
NetcPlus ⁷⁴¹	SmartServer3 3.75	Windows 95/98/Nt 4.0/2000	SmartServer3 Denial of Service	Low	CyberNotes-2000-24

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
NetcPlus ⁷⁴²	SmartServer3 3.75	Windows 95/98/NT 4.0/2000	SmartServer3 Weak Encryption	Medium	CyberNotes-2000-24
Netegrity ⁷⁴³	SiteMinder 3.6, 4.0	Windows NT 4.0, Unix	SiteMinder Authentication Bypass	Medium	CyberNotes 2000-19
Netnation Communications Inc. ⁷⁴⁴	Secure Locate 2.0, 2.1	Unix	Secure Locate LOCATE_PATH Validation	Low	CyberNotes 2000-13
Netopia ⁷⁴⁵	Netopia 650-ST ISDN Router 3.3.2 firmware		Netopia ISDN Router Username/ Password Disclosure	Medium	CyberNotes-2000-24
Netopia ⁷⁴⁶	R9100 DSL Router 4.6.2, R3100-T Router v4.6		Netopia DSL Router	Medium	CyberNotes 2000-10
Netopia ⁷⁴⁷	Timbuktu Pro 2.0, 3.0		Timbuktu Pro Cleartext Username/ Password passing	Medium	CyberNotes 2000-02
Netopia ⁷⁴⁸	Timbuktu Pro Remote Control 5.2.1, 2.0		Netopia Timbuktu Pro 2.0 Denial of Service	Low	CyberNotes 2000-04
Netscape ⁷⁴⁹	Communicator 4.x	Windows 95/98/NT 4.0/2000, Unix	Netscape JavaScript-in-Cookies Vulnerability	Medium	CyberNotes 2000-08
Netscape ⁷⁵⁰	Enterprise 3.5.1C, 3.5.1G, 3.5.1I, 3.6 SP1, SP2, SP3; Fasttrack 3.0.1, 3.0.2; Messaging Server 3.01, 3.54, 3.56, 3.6, 4.1, 4.15, 4.15p1, 4.15p2; Collabra Server 3.53, 3.54	Windows NT, Unix	Netscape Administration Server Password Disclosure	Medium	CyberNotes 2000-14
Netscape ⁷⁵¹	Enterprise Server 3.x		Netscape Web Publishing Tags	High	CyberNotes 2000-06
Netscape ⁷⁵²	Messaging Server 4.15, 4.15p1, 4.15p2	Windows NT 4.0, Unix	Netscape Messaging Server E-mail Address Verification	Medium	CyberNotes-2000-21
Netscape ⁷⁵³	Navigator & Communicator 4.05-4.07, 4.0, 4.5, 4.5BETA, 4.51, 4.6, 4.61, 4.7, 4.72		Netscape SSL Certificate Warning Bypass	High	CyberNotes 2000-10
Netscape ⁷⁵⁴	Netscape 4.73 and below without Personal Security Manager		Netscape Inconsistent Warning Messages	Medium	CyberNotes 2000-11
Netscape ⁷⁵⁵	Netscape Certificate Management System 4.2; Netscape Directory Server 4.12	Windows NT 4.0	Netscape Servers Suite Heap Buffer Overflow	High	CyberNotes-2000-22
Netscape ⁷⁵⁶	Netscape Certificate Server 4.2; Netscape Directory Server 4.12	Windows NT 4.0	Netscape Servers Suite Denial of Service	Low	CyberNotes-2000-22
Netscape ⁷⁵⁷	Netscape Enterprise 4.0		Netscape Error 404 Page	High	CyberNotes 2000-06
Netscape ⁷⁵⁸	Netscape Enterprise Server 3.6SP2		Netscape Enterprise Server GET Request	High	CyberNotes 2000-05
Netscape ⁷⁵⁹	Netscape iCal 2.1Patch2	Unix	Netscape Multiple Vulnerabilities	High	CyberNotes-2000-21
Netscape ⁷⁶⁰	Netscape Navigator		Netscape FTP URL JavaScript	High	CyberNotes 2000-06
Netscape ⁷⁶¹	Netscape Navigator v4.5		Buffer Overflow Vulnerability	High	CyberNotes 2000-01
Netscape ^{762, 763}	Communicator 4.05-4.08, 4.0, 4.5-4.51, 4.6-4.61, 4.72-4.74	Windows 95/98/NT 4.0/2000, Unix	Netscape URL File Read and Listening Socket Vulnerabilities	Medium/High	CyberNotes 2000-16, CyberNotes 2000-17
Netscape ^{764, 765, 766, 767}	Communicator 4.05- 4.08, 4.0, 4.5, 4.5BETA, 4.51, 4.6, 4.61, 4.7-4.73; Mozilla Browser M15		Netscape Communicator JPEG-Comment Heap Overwrite	High	CyberNotes 2000-15, CyberNotes 2000-17
Netscape ^{768, 769}	Netscape Communicator 4.6, 4.7		URL Variable Overflow Vulnerability	Medium/High	CyberNotes 2000-01
Netscape ^{770, 771}	Netscape Professional Services FTP Server 1.3.6	Unix	Netscape Professional Services FTP Server	High	CyberNotes 2000-13, CyberNotes 2000-14

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Netwin ⁷⁷²	DMail 2.5d	Windows 9/98/NT 4.0, Unix, MacOS 9.0	Netwin Dmailweb Server utoken Buffer Overflow	High	CyberNotes 2000-09
Netwin ⁷⁷³	DMailWeb & CWMail 2.53, 2.6g, 2.6I, 2.6j		DMailWeb & CWMail Multiple Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-13
Netwin ⁷⁷⁴	DNews 5.3	Windows 9/98/NT 4.0, Unix, MacOS 9.0	Netwin DNews News Server Buffer Overflow	High	CyberNotes 2000-10
Netwin ⁷⁷⁵	DSMTP Server 2.7q	Windows NT/2000, Unix	Netwin DSMTP Remote Buffer Overflow	High	CyberNotes 2000-12
Netwin ⁷⁷⁶	Netauth 4.2 and previous	Windows 95/NT 4.0, MacOS 9.0, Unix	Netwin Netauth Directory Traversal	Medium	CyberNotes 2000-17
Netwin ⁷⁷⁷	Netwin DMailWeb & CWMail 2.6g		DMailWeb & CWMail Denial of Service	Medium/High (High if DDoS best-practices not in place)	CyberNotes 2000-13
Network Associates, Inc. ⁷⁷⁸	Gauntlet for NT 5.0 (unpatched, and with hotfixes 1,2,3) Gauntlet for NT 5.5 (unpatched, and with SP1 and hotfixes 1,2,3,4)	Windows NT	Gauntlet NAT Mishandling	Medium	CyberNotes 2000-11
Network Associates, Inc. ⁷⁷⁹	PGP 5.0	Unix	PGP Insecure Key Generation	Medium	CyberNotes 2000-11
Network Associates, Inc. ⁷⁸⁰	Gauntlet 4.1, 4.2, 5.0, and 5.5 running Webshield CyberPatrol daemon; WebShield 100 series E-ppliance, WebShield 300 series E-ppliance, WebShield For Solaris 4.0	Unix	Gauntlet and Webshield CyberPatrol Buffer Overflow	High	CyberNotes 2000-11
Network Associates, Inc. ⁷⁸¹	Net Tools PKI Server 1.0		Net Tools PKI Unauthenticated Access and Buffer Overflow Vulnerabilities	High	CyberNotes 2000-13
Network Associates, Inc. ⁷⁸²	Net Tools PKI Server 1.0, 1.0Hotfix1, 1.0Hotfix2	Windows NT 4.0	Net Tools Multiple Vulnerabilities	Low	CyberNotes 2000-16
Network Associates, Inc. ⁷⁸³	Netshield 4.5, VirusScan for Windows NT 4.5	Windows NT 4.0/2000	VirusScan/NetShield AutoUpgrade Executable Verification	High	CyberNotes 2000-14
Network Associates, Inc. ⁷⁸⁴	PGP 5.5.3x-6.5.3i	Windows 95/98/NT 4.0/2000	PGP ADK Insertion	Medium/High	CyberNotes 2000-17
Network Associates, Inc. ⁷⁸⁵	PGP Certificate Server Version 2.5.0 & 2.5.1 for Solaris & Windows	Windows NT/2000, Unix	PGP Certificate Server Denial of Service	Low	CyberNotes 2000-12
Network Associates, Inc. ⁷⁸⁶	Sniffer Agent 3.0.10	Windows NT	Sniffer Agent Multiple Vulnerabilities	High	CyberNotes-2000-23
Network Associates, Inc. ⁷⁸⁷	WebShield SMTP 4.5	Windows NT 4.0/2000	WebShield SMTP Content Filter Bypass And SMTP Invalid Outgoing Recipient Field Denial of Service	Medium	CyberNotes-2000-24
Network Associates, Inc. ⁷⁸⁸	Webshield SMTP 4.5.44 Management Tool	Windows NT 4.0 Server	Webshield Configuration Modification Vulnerability	Medium	CyberNotes 2000-11
NetworkICE ⁷⁸⁹	BlackICE Defender 2.1 and previous; BlackICE Agent 2.0.23 and previous	Windows 95/98/NT 4.0/2000	BlackICE High UDP Port Block Delay	High	CyberNotes 2000-13
NetworkICE ⁷⁹⁰	ICECap Manager 2.0.23 and previous	Windows NT 4.0	NetworkICE ICECap Manager Default Username and Password	Medium	CyberNotes 2000-10

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
NetZero ⁷⁹¹	ZeroPort 3.0 and previous	Windows 95/98/NT 4.0/2000	ZeroPort Weak Encryption Method	Medium	CyberNotes 2000-15
Nevis Systems ⁷⁹²	All-Mail 1.1	Windows NT 4.0/2000	All-Mail Buffer Overflow	High	CyberNotes-2000-21
Nokia ⁷⁹³	Nokia IP440 1.0		Nokia IP440 Remote Denial of Service	High (High if DDoS best-practices not in place)	CyberNotes-2000-25
Nortel Networks ⁷⁹⁴	Contivity 1.0		Contivity Metacharacter CGIproc Crash	Low	CyberNotes 2000-02
Nortel Networks ⁷⁹⁵	Netgear ISDN 348.0RH, 328.0RT		Nortel Netgear ISDN RH348 and RT328 Denial Of Service	Low	CyberNotes 2000-05
Nosque Workshop ⁷⁹⁶	MsgCore 1.9		MsgCore SMTP Denial of Service	Low	CyberNotes 2000-02
Novell ⁷⁹⁷	Border Manager 3.0, 3.5		Border Manager URL Rule Restriction Bypass	Medium	CyberNotes 2000-14
Novell ⁷⁹⁸	Border Manager 3.0, 3.5		Border Manager User Impersonation	Medium	CyberNotes 2000-14
Novell ⁷⁹⁹	GroupWise 5.2, 5.5		GWWEB.EXE Vulnerabilities	Low	CyberNotes 2000-01
Novell ⁸⁰⁰	Groupwise Web Access 5.5 Enhancement Pack		Novell GroupWise 5.5 Enhancement Pack Denial of Service	Low	CyberNotes 2000-03
Novell ⁸⁰¹	Netware 5.0, 5.1; Netscape Enterprise Server for NetWare 4/5 4.1.1, 4/5 5.0		Netscape Enterprise Server for Netware Buffer Overflow	High	CyberNotes 2000-13
Novell ⁸⁰²	Netware 5.0SP5		Netware Port 40193 Denial of Service	Low	CyberNotes 2000-14
Novell ⁸⁰³	Netware 5.1 (any system running on the top of Netware system with http remote administration)		Netware 5.1 Remote Administration Buffer Overflow Vulnerability	High	CyberNotes 2000-08
Novell ⁸⁰⁴	Novell Client 3.1; Symantec Norton AntiVirus 5.0	Windows 95/98	Norton Antivirus with Novell Client Autoprotection Disabling	High	CyberNotes 2000-16
Novell ^{805, 806}	Border Manager 3.0, 3.5		Novell Border Manager Audit Trail Proxy Denial of Service	Low	CyberNotes 2000-03, CyberNotes 2000-04
NT.Mailserver.com ⁸⁰⁷	NTMail 5.0	Windows NT 4.0	NTMail Server 5.x Proxy Access	Medium	CyberNotes 2000-10
NullSoft ⁸⁰⁸	Winamp 2.10		Winamp Playlist Vulnerability	High	CyberNotes 2000-01
NullSoft ⁸⁰⁹	Winamp 2.64 and previous	Windows 95/98/NT 4.0/2000	Nullsoft Winamp M3U Playlist Buffer Overflow	High	CyberNotes 2000-15
Oatmeal Studios ⁸¹⁰	MailFile 1.10		MailFile Arbitrary File Disclosure	Medium	CyberNotes-2000-21
Oliver Fourdan ⁸¹¹	Xfce 3.5, 3.5.1	Unix	Xfce Port Display	Medium	CyberNotes-2000-23
Omnis ⁸¹²	Omnis Rapid Application Development	Windows NT/2000, Unix	Omnis Weak Database Encryption	Low	CyberNotes 2000-12
ON Technology ⁸¹³	Meeting Maker 1.0-6.0	Multiple Systems	Meeting Maker Weak Password Encryption	Medium	CyberNotes 2000-09
OpenBSD ⁸¹⁴	OpenBSD 2.3-2.7.3	Unix	Multiple Vendor BSD fstat Format String	Medium	CyberNotes 2000-20
OpenBSD ⁸¹⁵	OpenBSD 2.0-2.6	Unix	OpenBSD Pending ARP Request Remote Denial of Service	Low	CyberNotes 2000-20
OpenBSD ⁸¹⁶	OpenBSD 2.3-2.7	Unix	OpenBSD photurisd Format String	High	CyberNotes 2000-20
OpenBSD ⁸¹⁷	OpenBSD 2.6, 2.7	Unix	OpenBSD Xlock Data overflow	High	CyberNotes-2000-21
OpenBSD ^{818, 819}	OpenSSH 2.2.x	Unix	OpenSSH Client Unauthorized Remote Forwarding	Medium	CyberNotes-2000-23
OpenSSH ⁸²⁰	OpenSSH 2.1.1 and below with UseLogin option enabled	Unix	OpenSSH Remote Root Compromise	High	CyberNotes 2000-12
Oracle ⁸²¹	Oracle Listener 7.3.4, 8.0.6, 8.1.6		Oracle Listener Input Validation	High	CyberNotes-2000-22
Oracle ⁸²²	Oracle Oracle8i 8.1.6; Oracle Internet Directory 2.0.6	Unix	Oracle Internet Directory Oidldap	Medium	CyberNotes-2000-22

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Oracle ⁸²³	Oracle Web Listener 4.0.x on Windows NT	Windows NT	Oracle Web Listener Vulnerabilities	High	CyberNotes 2000-06
Oracle ⁸²⁴	Oracle Web Listener 4.07 & 4.0.8 for AIX	Unix	Web Listener Denial of Service	Low	CyberNotes 2000-14
Oracle ⁸²⁵	Oracle8i 8.1.5	Unix	Oracle for Linux Installer	High	CyberNotes 2000-05
Oracle ⁸²⁶	Oracle8i 8.1.5	Unix	Oracle cmctl Buffer Overflow	Medium	CyberNotes-2000-24
OReilly Software ⁸²⁷	WebSite Pro 2.3.7 and previous	Windows 95/98/NT 4.0/2000	WebSite Pro Write Access	Medium	CyberNotes 2000-18
OReilly Software ⁸²⁸	WebSite Professional 2.3.18, 2.4, 2.4.9	Windows 95/98/NT 4.0/2000	WebSite GET Buffer Overflow	High	CyberNotes 2000-15
OReilly Software ⁸²⁹	Website Professional 2.3.18, 2.4, 2.4.9	Windows 95/98/NT 4.0/2000	WebSite 'webfind.exe' Buffer Overflow	High	CyberNotes 2000-15
Padl Software ⁸³⁰	nss_ldap Build 105, 113, 85	Unix	nss_ldap Local Denial of Service	Low	CyberNotes-2000-22
Palm ⁸³¹	Palm OS 3.5.2		Palm OS Weak Encryption	Medium	CyberNotes 2000-20
Panda Software ⁸³²	Panda Antivirus for NetWare 2.0		Panda Remote Unauthenticated Administration	High	CyberNotes 2000-13
Panda Software ⁸³³	Panda Security 3.x	Windows 9x	Panda Security 3.0 Multiple Vulnerabilities	Medium	CyberNotes 2000-08
PassWD ⁸³⁴	PassWD 1.2	Windows NT/2000	PassWD Weak Encryption	Medium	CyberNotes 2000-12
Patrick Powell ⁸³⁵	LPRng 3.6.1-3.6.15	Unix	LPRng Incorrect Installation Permissions	High	CyberNotes 2000-14
PCCS-Linux ⁸³⁶	MySQL Database Admin Tool 1.2.3, 1.2.4	Unix	MySQL Database Admin Tool Username/Password Exposure	Medium	CyberNotes 2000-16
PDGSoft ⁸³⁷	PDGSoft Shopping Cart	Windows NT/Unix	PDGSoft Remote Buffer Overflow Vulnerability	High	CyberNotes 2000-11
PeleSoft ⁸³⁸	NetSnap 1.2	Windows 95/98/NT 4.0/2000	NetSnap Buffer Overflow	High	CyberNotes-2000-23
Phorum ⁸³⁹	Phorum 3.1-3.2.7		Phorum PHP Configuration Disclosure	Medium	CyberNotes-2000-24
Phorum ⁸⁴⁰	Phorum 3.1-3.2.8		Phorum Arbitrary File Read	Medium	CyberNotes-2000-24
PHP Development Team ⁸⁴¹	PHP (any PHP program which provides file upload capability)		PHP Upload Arbitrary File Disclosure	Medium	CyberNotes 2000-18
PHP Development Team ⁸⁴²	PHP 3.0.14		PHP Path Reveal	Low	CyberNotes 2000-12
PHP Development Team ⁸⁴³	PHP v3.00; 3.0.1; 3.0.10, 11, 12, 13; 3.0.2 through 3.0.9		'Safe_mode' Failure Vulnerability	High	CyberNotes 2000-01
PHPix ⁸⁴⁴	PHPix 1.0-1.0.2		PHPix Directory Traversal	Medium	CyberNotes-2000-21
Piranha ⁸⁴⁵	Piranha		Piranha Weak Password Security	Low	CyberNotes 2000-12
PIX ⁸⁴⁶	PIX Firewall		PIX DMZ Denial of Service	High	CyberNotes 2000-07
Plus Technologies ⁸⁴⁷	LPPlus 3.2.2, 3.3	Unix	LPPlus Multiple Vulnerabilities	Low/High	CyberNotes 2000-19
Pocsag ⁸⁴⁸	Pocsag v2.05		Pocsag Remote Access Default Password	Medium	CyberNotes 2000-06
Poll It ⁸⁴⁹	Poll It v2.0		Poll It CGI Arbitrary Command	High	CyberNotes-2000-23
PostgreSQL ⁸⁵⁰	PostgreSQL 6.3.2, 6.5.3	Unix	PostgreSQL Cleartext Passwords	Medium	CyberNotes 2000-09
PowerScript ⁸⁵¹	PlusMail		PlusMail Password Changing	Medium	CyberNotes 2000-02
Pragma Systems ⁸⁵²	InterAccess TelnetD Server 4.0		InterAccess TelnetD Server 4.0 Buffer Overflow	High	CyberNotes 2000-04
Pragma Systems ⁸⁵³	InterAccess TelnetD Server 4.0		InterAccess TelnetD Server 4.0 Terminal Configuration	Low	CyberNotes 2000-04
Pragma Systems ⁸⁵⁴	TelnetServer 2000	Windows NT 2000	TelnetServer Rexec Buffer Overflow	Low	CyberNotes 2000-17
Progress ⁸⁵⁵	WebSpeed 3.0		Progress WebSpeed Administration Utility Configuration	Medium	CyberNotes 2000-03
PTlink Services ⁸⁵⁶	PTlink IRCd 3.5.3, IRC Services 1.8.1	Unix	PTlink IRCd and Services Denial of Service	Low	CyberNotes-2000-24
QNX Software Systems Ltd. ⁸⁵⁷	QSSL Voyager 2.01B		Voyager Webserver Multiple Vulnerabilities	Medium	CyberNotes 2000-18
QNX System Software, Limited (QSSL) ⁸⁵⁸	QSSL QNX 4.25A	Unix	QNX crypt() Vulnerability	Medium	CyberNotes 2000-08

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Quake ⁸⁵⁹	Quake War Utilities 1.1		Packet Amplifier Vulnerability	Low	CyberNotes 2000-01
Qualcomm ⁸⁶⁰	Eudora 4.2, 4.3	Windows 95/98/NT 4.0	Eudora 4.2/4.3 Warning Message Circumvention	High	CyberNotes 2000-09
Qualcomm ⁸⁶¹	Eudora Pro, Eudora Light 3.0		Qualcomm Eudora Pro Long Filename Attachment	Low	CyberNotes 2000-10
Qualcomm ⁸⁶²	Qpopper 2.53	Unix	Qpopper Remote Shell Vulnerability	High	CyberNotes 2000-11
Qualcomm ⁸⁶³	Qpopper 3.0; 3.0beta (1 through 29)		Qpopper Mail Buffer Overflow	Medium	CyberNotes 2000-02
Rainbow Technologies, Inc. ⁸⁶⁴	iKey 1000	Windows 95/98/NT	IKey Administrator Access and Data Compromise	High	CyberNotes 2000-15
Ranson Johnson ⁸⁶⁵	Combination Mail-to and Credit Card Orderform 1.9 and previous	Windows NT 4.0, Unix	Mailto.cgi Address	High	CyberNotes 2000-19
Ranson Johnson ⁸⁶⁶	MailForm 2.0	Windows NT, Unix	MailForm 2.0 XX-attach_file	Medium	CyberNotes 2000-19
RapidStream ⁸⁶⁷	RapidStream 2000, 4000, 6000, 8000		RapidStream Unauthenticated Remote Command Execution	High	CyberNotes 2000-17
Real Networks ⁸⁶⁸	Real Networks Real Server 7, 7.01, G2 1.0, 8 BETA		Real Server HTTP Port Denial of Service	Low	CyberNotes 2000-12
Real Networks ⁸⁶⁹	Real Server Pro, Intranet, Plus, Basic, 7.0, G2 1.0,	Windows, Unix	RealServer Port 7070 Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-08
Real Networks ⁸⁷⁰	RealMedia Server v5.0		Remote Denial of Service Vulnerability	Low	CyberNotes 2000-01
Real Networks ⁸⁷¹	RealPlayer for Windows 6.0, 7.0		RealPlayer Location Buffer Overflow	High	CyberNotes 2000-07
Real Networks ⁸⁷²	RealServer 5.0, 6.0x, 7.0		RealServer Memory Contents Disclosure	High	CyberNotes-2000-24
RealMedia ⁸⁷³	RealServer		RealServer Internal IP Address	Medium	CyberNotes 2000-06
Recourse Technologies ⁸⁷⁴	ManTrap 1.6.1		ManTrap Multiple Vulnerabilities	Low/Medium	CyberNotes-2000-23
RedHat ⁸⁷⁵	Glnt 2.6.2	Unix	RedHat Glnt/tmp Symlink	Medium/High	CyberNotes 2000-19
RedHat ⁸⁷⁶	Linux 4.0-4.2, 5.0-5.2, 6.0-6.2; TurboLinux 6.0.2 and earlier	Unix	RedHat Man Buffer Overrun	High	CyberNotes 2000-05
RedHat ⁸⁷⁷	Linux 5.2, 6.0-6.2, (i386, alpha, sparc), 6.2E	Unix	RedHat Mgetty Sendfax	High	CyberNotes 2000-19
RedHat ⁸⁷⁸	Linux 5.2, 6.2, i386, alpha, sparc	Unix	RedHat Xpdf Embedded URL	High	CyberNotes 2000-19
RedHat ⁸⁷⁹	Linux 6.0-6.2 sparc, i386, alpha	Unix	RedHat Linux diskcheck Race Condition	High	CyberNotes-2000-25
RedHat ⁸⁸⁰	Linux 6.1 i386	Unix	RedHat Tmpwatch Recursive Write Denial of Service	Low	CyberNotes 2000-19
RedHat ⁸⁸¹	Linux 6.2 alpha, 6.2.i386, 6.2 sparc	Unix	RedHat Piranha Virtual Server Package Passwd.php3 and Default Account and Password	High	CyberNotes 2000-09
RedHat ⁸⁸²	Linux 6.2 alpha, i386, sparc, 7.0	Unix	RedHat Linux Ping Buffer Overflow	Medium	CyberNotes-2000-21
RedHat ⁸⁸³	Linux kernel 2.1.x, 2.2.x, 2.3.x	Unix	Linux knfsd Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-09
RedHat ⁸⁸⁴	PAM on Linux	Unix	Userhelper Vulnerability	High	CyberNotes 2000-01
RedHat ⁸⁸⁵	Powertools 6.1 and 6.2 i386, alpha, sparc	Unix	Multiple Imwheel Vulnerabilities	Low	CyberNotes 2000-14
RedHat ⁸⁸⁶	RedHat gkermit 1.0-3	Unix	Gkermit Setgid UUCP	Medium	CyberNotes 2000-13
RedHat ⁸⁸⁷	RedHat Linux 5.2, 6.0, 6.1, 6.2, i386, alpha, sparc, 6.2EE - i386, 7.0 i386	Unix	RedHat Pine Denial of Service	Medium	CyberNotes-2000-23

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
RedHat ⁸⁸⁸	RedHat Linux 6.2 sparc, i386, alpha BSD lpr 0.54-4	Unix	RedHat Lpr Arbitrary Command Execution	High	CyberNotes-2000-22
RedHat ⁸⁸⁹	RedHat restore 0.4b15	Unix	RedHat Restore Insecure Environment Variables	High	CyberNotes-2000-23
RedHat ⁸⁹⁰	rpc.lockd in Red Hat 6.1 & 6.2	Unix	RedHat rpc.lockd Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-12
RedHat ⁸⁹¹	University of Massachusetts scheme 3.2-11	Unix	Linux Umb-scheme World Writable	High	CyberNotes 2000-16
RedHat ⁸⁹²	University of Washington imapd 12.264	Unix	Univ. Of Washington imapd Buffer Overflow	Medium	CyberNotes 2000-08
RedHat and Debian ⁸⁹³	Linux	Unix	Multiple lpr/lpd Vulnerabilities	High	CyberNotes 2000-01
RedHat ^{894, 895}	Dump 0.4b15-1; Trustix Secure Linux 1.1	Unix	Multiple Vendor dump Insecure Environment Variables	High	CyberNotes-2000-22, CyberNotes-2000-23
RedHat ^{896, 897}	Linux 6.0, 6.1, 6.2.	Unix	Linux Usermode Denial of Service	High	CyberNotes 2000-18, CyberNotes-2000-23
Rit Research Labs ⁸⁹⁸	The Bat! 1.39		The Bat! X-BAT-FILES Vulnerabilities	Medium	CyberNotes 2000-05
Roaring Penguin Software ⁸⁹⁹	PPPoE 2.0-2.4	Unix	Roaring Penguin PPPoE Denial of Service	Low	CyberNotes-2000-25
Rob Flynn ⁹⁰⁰	Gaim 0.10.3, 0.10x	Unix	Gaim Remote Buffer Overflow	High	CyberNotes-2000-23
Robotex ^{901, 902}	Viking Server 1.0.6 Build 355 and prior	Windows 95/NT 4.0	Viking Server Buffer Overflow	High	CyberNotes 2000-18, CyberNotes 2000-19
Rockliffe ⁹⁰³	MailSite-HTTPMA/4.2.1.0	Windows NT	MailSite Remote Buffer Overflow	High	CyberNotes 2000-11
Roxen ⁹⁰⁴	WebServer 2.0.X	Unix	Roxen WebServer %00 Request File/Directory Disclosure	Medium	CyberNotes 2000-15
Samba ⁹⁰⁵	Samba 2.0.7	Unix	SAMBA SWAT Logging Failure and Symlink	High	CyberNotes-2000-22
Samba ⁹⁰⁶	Samba 2.0.7	Unix	Samba SWAT Logfile Permissions	High	CyberNotes-2000-23
Sambar Technologies ⁹⁰⁷	Sambar Server 4.3	Windows NT	Sambar Buffer Overflow	High	CyberNotes 2000-12
Sambar Technologies ⁹⁰⁸	Sambar Server 4.4Beta 3	Windows 95/98/NT 4.0	Sambar Server (BETA) Search CGI	Medium	CyberNotes 2000-19
Sambar Technologies ⁹⁰⁹	Sambar systems prior to 4.2 beta 8		Sambar Sensitive Information	Medium	CyberNotes 2000-05
Sambar Technologies ⁹¹⁰	Server 4.2beta 7 and older		Sambar Server Batch CGI	High	CyberNotes 2000-04
Sapporo Works ⁹¹¹	WinProxy 2.0, 2.0.1	Windows 95/98/NT 4.0/2000	WinProxy Buffer Overflow	High	CyberNotes 2000-13
Savant ⁹¹²	Savant Web Server v2.0		Denial of Service Vulnerability	Low	CyberNotes 2000-01
Savant ⁹¹³	Savant WebServer	Windows	Savant WebServer CGI Source Reveal	Low	CyberNotes 2000-12
SBC Communications ⁹¹⁴	Cayman DSL Router		Cayman DSL Router Password	Medium	CyberNotes 2000-06
SCO Secure Technologies Group ⁹¹⁵	UnixWare 7.0	Unix	Unixware /search97cgi/vtopic	Medium	CyberNotes 2000-19
SCO Secure Technologies Group ⁹¹⁶	Open Server 5.0.5		SCO OpenServer SNMPD Default Community	High	CyberNotes 2000-03
SCO Secure Technologies Group ⁹¹⁷	OpenServer 5.0-5.0.5		SCO MMDF Buffer Overflow	High	CyberNotes 2000-04
SCO Secure Technologies Group ⁹¹⁸	Unixware 7.0	Unix	Unixware SCOhelp HTTP Server Format String	High	CyberNotes 2000-20

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
SCO Secure Technologies Group ⁹¹⁹	UnixWare 7.0.0, 7.0.1	Unix	SCO PPP Buffer Overflow Privilege Escalation	Medium	CyberNotes 2000-02
SCO Secure Technologies Group ⁹²⁰	UnixWare 7.1	Unix	Remove Buffer Overflow Vulnerability	High	CyberNotes 2000-01
SCO Secure Technologies Group ⁹²¹	UnixWare 7.1	Unix	Local Pis and Mkpis File Creation Vulnerability	High	CyberNotes 2000-01
SCO Secure Technologies Group ⁹²²	UnixWare 7.1	Unix	Buffer Overflow Vulnerability	High	CyberNotes 2000-01
SCO Secure Technologies Group ⁹²³	UnixWare 7.1	Unix	Buffer Overflow Vulnerability	High	CyberNotes 2000-01
SCO Secure Technologies Group ⁹²⁴	UnixWare 7.1, 7.1.2	Unix	SCO Unixware ARCserver /tmp symlink	High	CyberNotes 2000-04
Seattle Labs ⁹²⁵	Emurl 2.0	Windows NT 4.0	Seattle Lab Emurl 2.0 Email Account Access	Medium	CyberNotes 2000-10
Sebastian Kienzl ⁹²⁶	muh 2.05d		Muh Format String	High	CyberNotes 2000-19
Sendmail ⁹²⁷	Sendmail 8.10.1 and below with Linux 2.2.15 and below		Sendmail Linux Capabilities	High	CyberNotes 2000-12
Sendmail Inc. ⁹²⁸	Sendmail 8.9.x		Sendmail Multiple Unsafe Fgets()	Low/Medium	CyberNotes 2000-09
Sendmail, Inc. ⁹²⁹	Sendmail (all versions)		Denial of Service Vulnerability	Low	CyberNotes 2000-01
Shadow Op Software ⁹³⁰	Dragon Server 1.0 & 2.0	Windows NT/2000	Dragon Server Multiple Buffer Overflows	High	CyberNotes 2000-12
Shadow Op Software ⁹³¹	Dragon Server 1.0, 2.0	Windows NT/2000	Dragon Server Multiple Denial of Service Vulnerabilities	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-13
Silicon Graphics, Inc. ⁹³²	Omron WorldView	Unix	Omron Worldview Root Compromise	High	CyberNotes 2000-17
Silicon Graphics, Inc. ⁹³³	Irix 5.2, 5.3, 5.3XFS, 6.0, 6.01, 6.01XFS, 6.1, 6.2	Unix	IRIX Objectserver Vulnerability	Medium/High	CyberNotes 2000-07
Silicon Graphics, Inc. ⁹³⁴	IRIX 5.x, 6.x	Unix	AGI Fam Unauthorized Access	Medium	CyberNotes 2000-05
Silicon Graphics, Inc. ⁹³⁵	IRIX 6.2	Unix	Sound Player Security Vulnerability	High	CyberNotes 2000-01
Silicon Graphics, Inc. ⁹³⁶	IRIX 6.2-6.5.6	Unix	IRIX Performance Copilot	Medium	CyberNotes 2000-08
Silicon Graphics, Inc. ⁹³⁷	IRIX 6.5	Unix	Sgi InfoSearch fname	High	CyberNotes 2000-05
Silicon Graphics, Inc. ⁹³⁸	IRIX 6.5-6.5.7 Infosearch	Unix	IRIX Infosearch Vulnerability	Low	CyberNotes 2000-11
Silicon Graphics, Inc. ⁹³⁹	IRIX 6.2	Unix	IRIX libgl.so Buffer Overflow	High	CyberNotes 2000-16
Silicon Graphics, Inc. ⁹⁴⁰	IRIX 6.2, 6.3	Unix	IRIX Lpstat Buffer Overflow	High	CyberNotes 2000-16
Silicon Graphics, Inc. ⁹⁴¹	IRIX 6.2, 6.3	Unix	IRIX Dmplay Buffer Overflow	High	CyberNotes 2000-16
Silicon Graphics, Inc. ⁹⁴²	IRIX 6.2, 6.3	Unix	IRIX Gr_osview Buffer Overflow	High	CyberNotes 2000-16
Silicon Graphics, Inc. ⁹⁴³	IRIX 6.2-6.4	Unix	IRIX Xfs Truncate() Privilege Check	Medium	CyberNotes 2000-16
Silicon Graphics, Inc. ⁹⁴⁴	IRIX 6.5, 6.5.1, 6.5.2m, 6.5.3, 6.5.3f, 6.5.3m, 6.5.4, 6.5.6-6.5.8	Unix	IRIX Inpview Race Condition	High	CyberNotes 2000-16
Silicon Graphics, Inc. ⁹⁴⁵	Workshop Debugger and Performance Tools 2.6 and lower	Unix	IRIX Cvconnect File Overwrite	High	CyberNotes 2000-13

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Silicon Graphics, Inc. ⁹⁴⁶	IRIX 5.2, 5.3, 5.3XFS, 6.0, 6.0.1, 6.0.1XFS, 6.1-6.5, 6.5.1, 6.5.2m, 6.5.3, 6.5.3f, 6.5.3m, 6.5.4-6.5.8	Unix	IRIX Telnetd Environment Variable Format String	High	CyberNotes 2000-17
Slackware ⁹⁴⁷	Linux 7.0.0 and 7.1.0.	Unix	Linux Multiple Buffer Overflow Vulnerabilities	Low	CyberNotes 2000-17
Slashcode ⁹⁴⁸	Slashcode 1.0.8 and previous		Slashcode Default Admin Password	High	CyberNotes 2000-20
SmartStuff ⁹⁴⁹	FoolProof Security 3.9	Windows 95/98/ME	FoolProof Security Program Restriction Bypass	Medium	CyberNotes-2000-25
SmartWin Technology ⁹⁵⁰	CyberOffice Shopping Cart 2.0	Windows NT 4.0/2000	CyberOffice Shopping Cart Client Information Disclosure	Medium	CyberNotes 2000-20
SmartWin Technology ⁹⁵¹	CyberOffice Shopping Cart 2.0	Windows NT 4.0/2000	CyberOffice Shopping Cart Price Modification	Medium	CyberNotes 2000-20
Software Composition Group ⁹⁵²	Oscar Nierstrasz Htgrep	Unix	Htgrep CGI Arbitrary File Viewing	Medium	CyberNotes 2000-17
Software602 ⁹⁵³	602Pro LAN SUITE Buffer Overflow	Windows 95/98/NT 4.0/2000	602Pro LAN SUITE Buffer Overflow	High	CyberNotes-2000-24
Sojourn ⁹⁵⁴	Sojourn Search Engine		Sojourn Directory Traversal	High	CyberNotes 2000-06
SolutionScripts ⁹⁵⁵	HomeFree CGI package		CGI Package Vulnerability	Low	CyberNotes 2000-01
SonicWALL ⁹⁵⁶	SOHO 4.0.0, 5.0.0		SOHO Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes-2000-24
SourceForge ⁹⁵⁷	Pam_mysql 0.1-0.4	Unix	Pam_mysql Authentication Input Validation	High	CyberNotes-2000-22
SourceGear Corporation ⁹⁵⁸	Concurrent Versions System (CVS) 1.10.		CVS Local Denial of Service	Low	CyberNotes 2000-09
SSH Communications Security ⁹⁵⁹	SSH 1.2.27	Unix	SSH 1.2.27 Kerberos Ticket Cache Exposure	Medium	CyberNotes 2000-14
Stalker Software ⁹⁶⁰	CommuniGate Pro 3.3.2		CommuniGate Pro E-mail Address Verification	Low	CyberNotes-2000-21
Stalkerlab ⁹⁶¹	Mailers 1.1.2	Windows NT 4.0	Mailers 1.1.2 CGI Mail Spoofing	Medium	CyberNotes 2000-18
Standard & Poor ⁹⁶²	ComStock 4.2.4		Standard & Poor's ComStock Machine Vulnerabilities	Medium	CyberNotes 2000-07
Sun and other products which use the FlexLM license management system ⁹⁶³	GLOBEtrrotter FLEXlm 6.1; Sun Workshop 5.0; Sun Solaris 2,6, 2.6_X86; 2.7, 2.7_X86		FlexLM Symlink	High	CyberNotes 2000-04
Sun Microsystems, Inc. ⁹⁶⁴	HotJava Browser 3.0	Windows 98/NT 4.0, MacOS 8.0, Unix	Sun HotJava Browser Arbitrary DOM Access	Medium	CyberNotes-2000-22
Sun Microsystems, Inc. ⁹⁶⁵	Netscape Communicator 4.75; Microsoft Internet Explorer 5.0.1 for Windows 98, NT 4.0	Windows 95/98/NT 4.0/2000, Unix	Sun Compromised Browser Certificates	High	CyberNotes-2000-22
Sun Microsystems, Inc. ⁹⁶⁶	Solaris 2.7 DMI service provider daemon (dmispd)	Unix	Denial of Service Vulnerability	Low	CyberNotes 2000-01
Sun Microsystems, Inc. ⁹⁶⁷	Solaris 6.0, 7.0	Unix	Solaris Lpset Buffer Overflow	High	CyberNotes 2000-09
Sun Microsystems, Inc. ⁹⁶⁸	Solaris 7.0, 7.0_x86	Unix	Solaris Xsun Buffer Overrun	High	CyberNotes 2000-09
Sun Microsystems, Inc. ⁹⁶⁹	Solaris 7.0, 7.0_x86	Unix	Solaris Lp -d Option Buffer Overflow	High	CyberNotes 2000-09

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Sun Microsystems, Inc. ⁹⁷⁰	Solaris 8 sun4u	Unix	Solaris ufsrestore Buffer Overflow	High	CyberNotes 2000-12
Sun Microsystems, Inc. ⁹⁷¹	Sun Java HotSpot Performance Engine 1.0, 1.0.1; Sun JDK (Linux Production Release) 1.2.2_05, 1.2.2_005 Sun JDK (Solaris Production Release) 1.1.6, 1.1.7B, 1.1.8_10, 1.2.1; Sun JDK (Solaris Reference Release) 1.1.6_007, 1.1.7B_005, 1.1.8_002, 1.2.1_003, 1.2.2_004; Sun JDK (Windows Production Release) 1.1.6_007, 1.1.7B_005, 1.1.8_002, 1.2.1_003, 1.2.2_004	Windows 98/98/NT, Unix	Sun JDK/JRE Disallowed Class Loading	Medium	CyberNotes-2000-25
Sun Microsystems, Inc. ⁹⁷²	Sun Java Web Server 1.1.3, 2.0	Windows NT 4.0, Unix	Sun Java Web Server Web Admin / Bulletin Board	High	CyberNotes 2000-17
Sun Microsystems, Inc. ⁹⁷³	AnswerBook2 1.3x, 1.4-1.4.2	Unix	AnswerBook2 Remote Command Execution and Administration Interface Access Vulnerabilities	High	CyberNotes 2000-16
Sun Microsystems, Inc. ⁹⁷⁴	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Unix	Solaris Netpr Buffer Overflow	High	CyberNotes 2000-10
Sun Microsystems, Inc. ⁹⁷⁵	Solaris 7	Unix	Solaris BIND Vulnerability	High	CyberNotes 2000-07
Sun Microsystems, Inc. ⁹⁷⁶	Solaris 7, 8	Unix	Solaris /var/partition Exploitation	Low	CyberNotes 2000-02
Sun Microsystems, Inc. ⁹⁷⁷	StarOffice 5.1	Unix	Star Office Buffer Overflow Vulnerabilities	Medium	CyberNotes 2000-08
Sun Microsystems, Inc. ⁹⁷⁸	StarScheduler/StarOffice 5.1	Unix	StarScheduler/ StarOffice Denial of Service and Arbitrary File Read Vulnerabilities	High	CyberNotes 2000-05
Sun Microsystems, Inc. ⁹⁷⁹	Sun Java Web Server 1.1.3, 2.0	Windows NT 4.0, Unix	Sun Java Web Server	High	CyberNotes 2000-14
Sun Microsystems, Inc. ^{980, 981}	Solaris 2.5, 2.5_x86, 2.5.1, 2.5.1_ppc, 2.5.1_x86, 2.6, 2.6_x86, 2.7, 2.7_x86	Unix	Sadmind Buffer Overflow Vulnerability	High	CyberNotes 2000-01
Sun Microsystems, Inc. ⁹⁸²	Solaris AT&T's Framed Access Command Environment (FAC)	Unix	Chkperm Buffer Overflow Vulnerability	High	CyberNotes 2000-01
Sun-Netscape Alliance ⁹⁸³	iPlanet Web Server 4.x	Windows NT 4.0, Unix	iPlanet Webserver .html Buffer Overflow	Low/High	CyberNotes-2000-22
SuSE ⁹⁸⁴	Linux 6.0-6.4	Unix	SuSE Linux Arbitrary File Deletion	Medium	CyberNotes 2000-09
SuSE ⁹⁸⁵	Linux 6.0-6.4, 7.0	Unix	SuSE in.identd Denial of Service	Low	CyberNotes-2000-24
SuSE ⁹⁸⁶	Linux 6.2-6.4, 7.0	Unix	SuSE ypbind-mt Format String	High	CyberNotes-2000-21
SuSE ⁹⁸⁷	Linux 6.3, 6.1	Unix	SuSE Make Root Compromise Vulnerability	High	CyberNotes 2000-03
SuSE ⁹⁸⁸	Linux 6.3, 6.4 Apache 1.3.9/12	Unix	SuSE Apache CGI Source Code Viewing	Medium	CyberNotes 2000-18
SuSE ⁹⁸⁹	Linux 6.3, 6.4	Unix	Linux Installed Package Disclosure	Medium	CyberNotes 2000-20
SuSE ⁹⁹⁰	Linux 6.3-6.4	Unix	Tnef 0-123 Mail Decoder File Overwrite	High	CyberNotes 2000-14
SuSE ⁹⁹¹	Linux 6.4 Apache 1.3.12	Unix	SuSE Apache WebDAV Directory	Medium	CyberNotes 2000-18
SuSE ⁹⁹²	S.u.S.E. Linux 6.3, 6.4	Unix	SuSE Gnomelib Buffer Overflow	Medium	CyberNotes 2000-09

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
SuSE ⁹⁹³	SuSE 6.1-6.4 Kernel 2.2.15	Unix	SuSE Kernel Denial of Service	Low	CyberNotes 2000-11
SuSE ⁹⁹⁴	SuSE 6.1-6.4 Kmulti 1.1.2	Unix	SuSE Kmulti Root Compromise	High	CyberNotes 2000-11
SuSE ⁹⁹⁵	SuSE 6.1-6.4 knfsd, all versions	Unix	SuSE String Parsing	High	CyberNotes 2000-16
Sybergen ⁹⁹⁶	Secure Desktop 2.1	Windows 95/98/NT 4.0	Secure Desktop Multiple Vulnerabilities	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-14
Sybergen ⁹⁹⁷	SyGate 2.0, 3.0, 3.1, 3.11	Windows 95/98/NT 4.0	SyGate Denial of Service	Low	CyberNotes 2000-14
Sybergen ⁹⁹⁸	SyGate 3.11, 2.0		SyGate Remote Administration Engine	High	CyberNotes 2000-03
Symantec ⁹⁹⁹	I-Gear 3.5.6	Windows NT 4.0	I-Gear for Microsoft Proxy long URL	Low	CyberNotes-2000-23
Symantec ¹⁰⁰⁰	Norton AntiVirus 2000		Remote Buffer Overflow Vulnerability	High	CyberNotes 2000-01
Symantec ¹⁰⁰¹	Norton Antivirus 5.02	Windows NT	Norton Antivirus Elevated Privileges	Medium	CyberNotes 2000-16
Symantec ¹⁰⁰²	Norton AntiVirus for Internet Email Gateways 1.0		Norton Gateways Buffer Overflow	Low	CyberNotes 2000-06
Symantec ¹⁰⁰³	Norton AntiVirus for Windows ME 2001	Windows ME	Norton AntiVirus 2001 _Restore Directory Virus Detection Bypass	Medium	CyberNotes-2000-22
Symantec ¹⁰⁰⁴	Norton Nav-Exchange 1.5 & 2.0	Windows NT/2000	Norton Nav-Exchange Unchecked Attachments & Buffer Overflow Vulnerabilities	High	CyberNotes 2000-12
Symantec ¹⁰⁰⁵	PcAnywhere 9.0		Symantec PcAnywhere Weak Encryption	Medium	CyberNotes 2000-07
Symantec ¹⁰⁰⁶	PcAnywhere versions 7.5-9.2		PcAnywhere Weak Password Encryption	Medium	CyberNotes 2000-11
Symantec ¹⁰⁰⁷	PCAnywhere32 8.0, 9.0	Windows 95/98/ NT 4.0/2000	PCAnywhere Denial of Service	Low	CyberNotes 2000-08
T.C.X DataKonsult ¹⁰⁰⁸	MySQL 3.20.x, 3.21.x, 3.22.x, 3.23.x		MySQL Authentication Algorithm	Medium	CyberNotes-2000-22
T.C.X DataKonsult ^{1009,1010}	MySQL 3.22.26-3.22.30, 3.23.8-10		MySQL Unauthenticated Remote Access	Medium	CyberNotes 2000-03, CyberNotes 2000-04
TalentSoft, Inc. ¹⁰¹¹	Web+ 4.x	Unix	TalentSoft Web+ Directory Traversal	High	CyberNotes 2000-08
TalentSoft, Inc. ¹⁰¹²	Web+ Application Server (Linux) 4.6	Unix	Web+ Example Script File Disclosure	Medium	CyberNotes 2000-20
TalentSoft, Inc. ¹⁰¹³	Web+ Client 4.6; Web+ Monitor 4.6; Web+ Server 4.6	Windows 95/98/NT 4.0, Unix	Web+ Multiple Disclosure Vulnerabilities	Medium	CyberNotes 2000-20
Tech-Source ¹⁰¹⁴	Raptor GFX PGX32 2.3.1	Unix	Raptor GFX Config Tool Vulnerabilities	High	CyberNotes 2000-16
Texas Imperial Software ¹⁰¹⁵	WFTPD 2.34, 2.40, 2.4.1, 2.4.1RC11	Windows 95/98/NT 4.0/2000	WFTPD Multiple Vulnerabilities	Low/Medium	CyberNotes 2000-15
Texas Imperial Software ¹⁰¹⁶	WFTPD 2.41RC14, 2.41RC14 Pro, 3.0Pro	Windows 95/98/3.1/NT 3.5/4.0/2000	Winsoc FTPd Directory Transversal	High	CyberNotes-2000-24
Texas Imperial Software ¹⁰¹⁷	WFTPD Pro 2.41 RC10, and prior	Windows NT 4.0/2000	WFTPD Denial of Service	Low	CyberNotes 2000-14
Texas Imperial Software ¹⁰¹⁸	WFTPD/WFTPD Pro versions 2.41 RC12 and prior	Windows	Multiple WFTPD Vulnerabilities	Low /Medium	CyberNotes 2000-18
The Ht://Dig Group ¹⁰¹⁹	Ht://Dig prior to 3.1.5 (multiple vendors)		ht://dig Arbitrary File Inclusion	Medium	CyberNotes 2000-05
TIS ¹⁰²⁰	Internet Firewall Toolkit 2.1		Firewall Toolkit Format String	High	CyberNotes-2000-22
Tony Greenwood ¹⁰²¹	WebWho+ v1.1		Remote Command Execution Vulnerability	High	CyberNotes 2000-01

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
TransSoft ¹⁰²²	Broker FTP Server 4.7.5.0	Windows 95/98/NT 4.0/2000	Broker FTP Directory Permissions	Medium	CyberNotes-2000-24
Trend Micro Systems ¹⁰²³	InerScan VirusWall v3.0.1		E-Mail Vulnerability	High	CyberNotes 2000-01
Trend Micro Systems ¹⁰²⁴	InterScan Virus Wall 3.0.1, 3.2.3, 3..3, 3.3	Windows NT 4.0	InterScan VirusWall uuencoded Remote Filename Buffer Overflow	High	CyberNotes 2000-09
Trend Micro Systems ¹⁰²⁵	InterScan VirusWall for Windows NT 3.4 and previous	Windows NT 4.0	InterScan VirusWall Shared Directory	High	CyberNotes-2000-24
Trend Micro Systems ¹⁰²⁶	PC-Cillian Anti-Virus v6.x		Remote Denial of Service Vulnerability	Low	CyberNotes 2000-01
Trend Micro Systems ^{1027, 1028}	OfficeScan 3.5		Trend Micro OfficeScan Denial of Service	High	CyberNotes 2000-05, CyberNotes 2000-06
TrendMicro Systems ¹⁰²⁹	InterScan version V3.32, build 1011, 1022	Windows NT	TrendMicro Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes 2000-08
Trlinux ¹⁰³⁰	Postaci Webmail 1.1.3	Unix	Postaci Webmail Password Disclosure	Medium	CyberNotes-2000-25
True North Software ¹⁰³¹	Internet Anywhere Mail Server 3.1.3		Internet Anywhere Mail Server Connection Overload	Low	CyberNotes 2000-03
True North Software ¹⁰³²	Internet Anywhere Mail Server 3.1.3		Internet Anywhere Mail Server RETR Denial of Service	Low	CyberNotes 2000-03
TrueNorth Software ¹⁰³³	Internet Anywhere Mail POP Server version 2.3.1		POP3 Buffer Overflow Vulnerability	High	CyberNotes 2000-01
Trustix ¹⁰³⁴	Trustix Secure Linux 1.1	Unix	Trustix Apache-SSL RPM Permissions	High	CyberNotes 2000-17
TServ Incorporated ¹⁰³⁵	RideWayPN 6.22	Windows 95/98/NT 4.0/2000	RideWayPN Denial of Service	Low	CyberNotes-2000-23
Tumbleweed ¹⁰³⁶	Messaging Management System (MMS) 4.3, 4.5, 4.6	Windows 95/98/NT 4.0/2000	Tumbleweed MMS No Default Password	Medium	CyberNotes 2000-16
TurboLinux ¹⁰³⁷	TurboLinux versions: 6.0.2 and earlier	Unix	TurboLinux Local Buffer Overflow	High	CyberNotes 2000-06
TurboLinux ¹⁰³⁸	TurboLinux versions: 6.0.2 and earlier	Unix	TurboLinux PAM Vulnerability	High	CyberNotes 2000-08
UltraScripts ¹⁰³⁹	UltraBoard 1.6	Windows, Unix	UltraBoard Directory Traversal	Low	CyberNotes 2000-09
Unify ¹⁰⁴⁰	eWave ServletExec		Unify ServletExec View Source Code	Medium	CyberNotes 2000-12
Unify ¹⁰⁴¹	eWave ServletExec 3.0, 3.0c	Windows 98/NT 4.0/2000, Unix	eWave ServletExec JSP Source Disclosure	Medium	CyberNotes-2000-24
Unify ¹⁰⁴²	eWave ServletExec 3.0c	Windows 98/NT 4.0/2000, Unix	eWave ServletExec Denial of Service	Low	CyberNotes-2000-22
Unify ¹⁰⁴³	eWave ServletExec 3.0c	Windows 98/NT 4.0/2000, Unix	Unify eWave ServletExec File Upload	High	CyberNotes-2000-22
University of Kansas ¹⁰⁴⁴	Lynx 2.7, 2.8, 2.8.3dev2x		Lynx Long URL Buffer Overflow	High	CyberNotes 2000-05
University of Minnesota ¹⁰⁴⁵	Gopherd 2.3.1p0 and previous	Unix	UMN Gopherd 'Halidate' Function Buffer Overflow	High	CyberNotes 2000-17
University of Minnesota ¹⁰⁴⁶	University of Minnesota gopherd 2.3, 2.3.1	Unix	Gopherd Remote Root Buffer Overflow	High	CyberNotes 2000-17
University of Washington ¹⁰⁴⁷	imapd 12.264 (This version is shipped with RedHat Linux 6.2)	Unix	Univ. Of Washington imapd Buffer Overflow	Medium	CyberNotes 2000-08
University of Washington ¹⁰⁴⁸	pico 3.7-4.3	Unix	University of Washington Pico File Overwrite	Medium	CyberNotes-2000-25
University of Washington ¹⁰⁴⁹	Pine 4.21	Unix	Pine "From:" Buffer Overflow	High	CyberNotes 2000-20

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
University of Washington ¹⁰⁵⁰	pop2d 4.46, 4.51, 4.54, 4.55	Unix	Pop2d Remote File Read	Medium	CyberNotes 2000-15
Unix ¹⁰⁵¹	BSD/OS 4.0.1; FreeBSD 3.4; Linux (with skkey-2.2-1 RPM)	Unix	FreeBSD and Linux S/Key & OPIE Database Compromise	Medium	CyberNotes 2000-02
Unix ¹⁰⁵²	Generic-NQS ver. 3.50.6; Generic-NQS ver. 3.50.7	Unix	Generai-NQS Local Root Compromise	High	CyberNotes 2000-06
Unix/Linux ¹⁰⁵³	abuse.man (webmanager kit)	Unix	Abuse.man CGI Security Vulnerability	High	CyberNotes 2000-06
Valve Software ¹⁰⁵⁴	Half-Life Dedicated Server 3.1 and previous	Unix	Half-Life Format String	High	CyberNotes-2000-22
Valve Software ^{1055, 1056}	Half-Life Dedicated Server 3.1 and previous	Unix	Half-Life Dedicated Server	High	CyberNotes-2000-21, CyberNotes-2000-22
Veritas Software ¹⁰⁵⁷	Volume Manager 3.0.2-3.0.4	Unix	Volume Manager File Permission	High	CyberNotes 2000-13
Virtual Vision ¹⁰⁵⁸	Virtual Vision FTP Browser 1.0		Virtual Vision FTP Browser	Medium	CyberNotes 2000-15
Visible Systems ¹⁰⁵⁹	Razor 4.1		Visible Systems Razor Password File	Medium	CyberNotes 2000-14
VMWare, Inc. ¹⁰⁶⁰	VMWare 1.1, 1.1.1, 1.1.2, 1.0.1, 1.0.2		VMWare Symlink File Overwrite	High	CyberNotes 2000-02
Volano LLC ¹⁰⁶¹	VolanoChat Pro 2.1	Unix	VolanoChatPro Local Password Disclosure	High	CyberNotes-2000-23
Voyant Technologies ¹⁰⁶²	Sonata v3.x on Solaris 2.x.; Sonata bridge OS/2 Warp	OS/2, Unix	Sonata Conferencing Multiple Vulnerabilities	High	CyberNotes-2000-23
VPNet Technologies ¹⁰⁶³	VPNos 3.0		VPNet VSU Source Routed Session	Medium	CyberNotes-2000-25
VPNet Technologies ¹⁰⁶⁴	VSU 100, 2000, 5000, 7500		VSU Multiple Vulnerabilities	Medium	CyberNotes-2000-25
VqSoft ¹⁰⁶⁵	vqServer 1.4.49	Windows, Unix	VqServer Long URL Denial of Service	Low	CyberNotes 2000-18
VqSoft ¹⁰⁶⁶	vqServer 1.9.9		VqServer Plaintext Password Storage	High	CyberNotes 2000-07
W3C ¹⁰⁶⁷	W3C httpd 3.0A		CERN HTTP Path Revealing	Low	CyberNotes 2000-02
WatchGuard ¹⁰⁶⁸	Firebox II	Unix	Firebox II Denial of Service	Low	CyberNotes 2000-17
WatchGuard ¹⁰⁶⁹	Firebox II 4.1, 4.5	Unix	Firebox II Denial of Service	Low/High (High if DDoS best-practices not in place)	CyberNotes-2000-24
WatchGuard Technologies, Inc. ¹⁰⁷⁰	SOHO Firewall 1.6, 2.1.3		Multiple SOHO Firewall Vulnerabilities	Low/High (High if DDoS best-practices not in place)	CyberNotes-2000-25
Web Plus ¹⁰⁷¹	Small HTTP Server 1.212	Windows NT/2000	Web Plus Small HTTP Buffer Overflow	High	CyberNotes 2000-12
WebTeacher ¹⁰⁷²	WebData 2.2 and previous	Windows 95/98/NT 4.0, Unix	WebTeacher WebData File Import	Medium	CyberNotes 2000-20
WebTV ¹⁰⁷³	WebTV		WebTV Vulnerability	Medium	CyberNotes 2000-01
West Street Software ¹⁰⁷⁴	LocalWEB HTTP Server 1.2	Windows 95/98/NT 4.0/2000	LocalWEB HTTP Buffer Overflow	High	CyberNotes 2000-14
WinGate ¹⁰⁷⁵	WinGate Home/Standard/Pro 4.0.1	Windows NT	Winsock Redirector Denial of Service	Low	CyberNotes 2000-20
WireSrv ¹⁰⁷⁶	IRC Server 5.0.7s	Windows	WireSrv IRC Server Character Flood Denial of Service	Low	CyberNotes 2000-14
WireSrv ¹⁰⁷⁷	IRC Server 5.0.7s	Windows 95/NT 4.0	WireSrv MOTD Read	Medium	CyberNotes 2000-15
Wired Community Software ¹⁰⁷⁸	WWWThreads 5.0b3 and prior		WWWThreads SQL Command Input	High	CyberNotes 2000-03
WMSoft, LLC ¹⁰⁷⁹	Phorum 3.0.x		Multiple Security Vulnerabilities	High	CyberNotes 2000-01
Worldtalk ¹⁰⁸⁰	WorldSecure Mail 4.3		WorldSecure Mail Virus File Signature Alteration	Medium	CyberNotes 2000-02

Vendor	Software Name	Operating System	Common Name	Risk*	CyberNotes Issue
Wormonline Software ¹⁰⁸¹	Jeremy Arnold Worm Webserver 1.0	Windows NT 4.0	Worm httpd Denial of Service and Directory Traversal	Medium	CyberNotes 2000-18
WQuinn ¹⁰⁸²	QuotaAdvisor 4.1	Windows NT 4.0/2000	WQuinn QuotaAdvisor 4.1 Disk Quota Bypass	Low	CyberNotes 2000-20
WQuinn ¹⁰⁸³	QuotaAdvisor 4.1	Windows NT 4.0/2000	QuotaAdvisor 4.1 Directory Listing Disclosure	Medium	CyberNotes-2000-21
Xfree ¹⁰⁸⁴	Xfree96 3.3.5, 3.3.6, 4.0	Unix	Multiple Vendor Xfree86 Malformed Packet Freeze	Low	CyberNotes 2000-11
XFree86 ¹⁰⁸⁵	XFCE 3.5.0-3.5.1	Unix	XFCE Local Xauthority Bypass	Medium	CyberNotes 2000-20
XFree86 ¹⁰⁸⁶	Xlib 3.3x	Unix	Xlib Buffer Overflow	High	CyberNotes-2000-21
XFree86 4.0 ¹⁰⁸⁷ (AKA XFree86 3.3.3.1)	Xterm, Eterm .0.8.10, Eterm 0.9	Unix	Xterm Denial of Service	Low	CyberNotes 2000-12
Xpdf ¹⁰⁸⁸	Xpdf 0.90	Unix	Xpdf Embedded URL	High	CyberNotes 2000-18
XS4ALL Data ¹⁰⁸⁹	SunFTP 1.0 Build 9		SunFTP Buffer Overflow and Denial of Service	Low	CyberNotes 2000-18
YaBB ¹⁰⁹⁰	YaBB 9.1.2000	Windows, Unix	YaBB Arbitrary File Read	Medium	CyberNotes 2000-19
YaBB ¹⁰⁹¹	YaBB 9.11.2000		YaBB Search.pl Arbitrary Command Execution	High	CyberNotes-2000-23
ZBSoft ¹⁰⁹²	ZBServer Pro edition for Windows NT	Windows NT	Buffer Overflow Vulnerability	High	CyberNotes 2000-01
Zedz Consultants ¹⁰⁹³	Ssh-1.2.27-8i.src.rpm 1.2.27-8i	Unix	Zedz Consultants ssh-1.2.27-8i.src.rpm Access Verification	High	CyberNotes 2000-10
Zeus Technologies ¹⁰⁹⁴	Zeus Web Server 3.1x, 3.3x		Zeus Web Server Null Terminated Strings	Medium	CyberNotes 2000-03
Zilron ¹⁰⁹⁵	Zilron StoreCreator 3.0		Zilron StoreCreator Remote Database Alter	Medium	CyberNotes 2000-12
Zone Labs ¹⁰⁹⁶	ZoneAlarm 2.1.10 & prior	Windows 95 2.1, 98 2.1, NT 4.0.2.1	ZoneAlarm Personal Firewall Port 67	Medium	CyberNotes 2000-09
Zope ¹⁰⁹⁷	Zope 2.1.1, 1.10.3		DTML Editing Vulnerability	High	CyberNotes 2000-01
Zope ¹⁰⁹⁸	Zope 2.2 beta 1 and below		Zope Remote Content Alerting	Medium	CyberNotes 2000-12
Zope ^{1099,1100}	Zope 2.1.x, 2.2 beta1	Unix	Zope DTML Templates And DTML Methods Remote Modification	Medium	CyberNotes 2000-13

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note 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 as a "High" threat.

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 2000 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	Issue discussed
Acid Shiver + Imacid	v1.0 + 1.0Mod	CyberNotes 2000-07
AOL Trojan		CyberNotes 2000-01
Asylum + Mini	v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1	CyberNotes 2000-10, CyberNotes 2000-12
AttackFTP		CyberNotes 2000-10
Backdoor/Doly.17		CyberNotes 2000-16
BackDoor-GZ		CyberNotes 2000-18
BackDoor-HC		CyberNotes 2000-18
Backdoor-HD		CyberNotes 2000-18
BCK/Sub7.Apocalypse		CyberNotes 2000-23
BF Evolution	v5.3.12	CyberNotes 2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes 2000-09, CyberNotes 2000-12
Bla	1.0-5.02, v1.0-5.03	CyberNotes 2000-06, CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes 2000-09
DeepThroat	v1.0 - 3.1 + Mod (Foreplay)	CyberNotes 2000-05
Delta Source	J0.5b-0.7	CyberNotes 2000-01
Donald Dick	1.52-1.55	CyberNotes 2000-01
Donald Dick 2		CyberNotes 2000-15
Donald Dick 2		CyberNotes 2000-15
Drat	v1.0 - 3.0b	CyberNotes 2000-09
Erap Estrada		CyberNotes 2000-18
FakeFTP	Beta	CyberNotes 2000-02
GIP		CyberNotes 2000-11
Girlfriend	V1.3x (including Patch 1 & 2)	CyberNotes 2000-05
Golden Retriever	v1.1b	CyberNotes 2000-10
Hack'A'tack	1.0-2000	CyberNotes 2000-01, CyberNotes 2000-06
Hooker-E		CyberNotes 2000-19
ICQ PWS		CyberNotes 2000-11

Trojan	Version	Issue discussed
ICQ PWS		CyberNotes 2000-11
ik97	v1.2	CyberNotes 2000-07
InCommand	v1.0 - 1.5	CyberNotes 2000-01, CyberNotes 2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes 2000-07, CyberNotes 2000-09
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes 2000-09, CyberNotes 2000-10
Intruder		CyberNotes 2000-01
Kaos	v1.1 - 1.3	CyberNotes 2000-10
Khe Sanh	v2.0	CyberNotes 2000-10
Kuang Original	0.34	CyberNotes 2000-01
Magic Horse		CyberNotes 2000-10
Matrix	v1.0 - 2.0	CyberNotes 2000-01, CyberNotes 2000-09
Mosaic	v2.00	CyberNotes 2000-16
MoSucker		CyberNotes 2000-06
Multijoke.B		CyberNotes 2000-15
Naebi	v2.12 - 2.39, v2.40	CyberNotes 2000-09, CyberNotes 2000-12
Netbus.153		CyberNotes 2000-17
Netbus.170		CyberNotes 2000-17
NetController	v1.08	CyberNotes 2000-07
NetSphere	v1.0 - 1.31337	CyberNotes 2000-06, CyberNotes 2000-09
Netsphere.Final		CyberNotes 2000-15
NetTrojan	1.0	CyberNotes 2000-06
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes 2000-07
NoDesk		CyberNotes 2000-14
Omega		CyberNotes 2000-12
Palm/Liberty-A		CyberNotes 2000-18
PALM_VAPOR.A		CyberNotes 2000-19
PE_MTX.A		CyberNotes 2000-18
Phaze Zero	v1.0b + 1.1	CyberNotes 2000-09
Prayer	v1.2 - 1.5	CyberNotes 2000-06, CyberNotes 2000-09
Prosiak	beta - 0.65 - 0.70 b5	CyberNotes 2000-09, CyberNotes 2000-12
Qaz.A	W32.HLLW.Qaz.A	CyberNotes 2000-16, CyberNotes 2000-20
QDel121		CyberNotes 2000-23
Revenger	1.0-1.5	CyberNotes 2000-12
Serbian Badman		CyberNotes 2000-12
Setup Trojan (Sshare) +Mod Small Share		CyberNotes 2000-06
ShadowPhyre	v2.12.38 - 2.X	CyberNotes 2000-06
ShitHeap		CyberNotes 2000-09
Snid	1-2	CyberNotes 2000-12
Softwarst		CyberNotes 2000-05
SubSeven	1.0-2.1c	CyberNotes 2000-01

Trojan	Version	Issue discussed
SubSeven	1.0-2.1Gold	CyberNotes 2000-02
SubSeven	DEFCON8 2.1 Backdoor	CyberNotes 2000-21
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes 2000-07
Trinoo		CyberNotes 2000-05
Troj/Simpsons		CyberNotes 2000-13
TROJ_BATMAN		CyberNotes 2000-20
TROJ_BLEBLA.A		CyberNotes 2000-24
TROJ_BLEBLA.B		CyberNotes 2000-24
TROJ_BLOODLUST		CyberNotes 2000-21
TROJ_BUTANO.KILL		CyberNotes 2000-19
Troj_Dilber		CyberNotes 2000-14
TROJ_ENERGY.A		CyberNotes 2000-24
TROJ_FELIZ		CyberNotes 2000-22
TROJ_ICECUBES.A		CyberNotes 2000-24
TROJ_IGMNUKE		CyberNotes 2000-20
TROJ_KILLME		CyberNotes 2000-20
TROJ_MSINIT.A		CyberNotes 2000-21
TROJ_MUSIC.A		CyberNotes 2000-24
TROJ_MYPICS.F		CyberNotes 2000-23
TROJ_NAVIDAD.A		CyberNotes 2000-23
TROJ_NAVIDAD.E		CyberNotes 2000-24
TROJ_ORION		CyberNotes 2000-24
TROJ_PERSONAL_ID		CyberNotes 2000-17
TROJ_POKEY.A		CyberNotes 2000-17
TROJ_ROCKET		CyberNotes 2000-22
TROJ_SCOOTER		CyberNotes 2000-19
TROJ_SHOCKWAVE.A		CyberNotes 2000-24
TROJ_SONIC		CyberNotes 2000-22
TROJ_SPAWNMAIL.A		CyberNotes 2000-18
TROJ_SUB7.214DC8		CyberNotes 2000-21
TROJ_SUB7.382883		CyberNotes 2000-21
TROJ_USSRHYMN.A		CyberNotes 2000-24
TROJ_VBSWG		CyberNotes 2000-16
Trojan/Anything		CyberNotes 2000-23
Trojan/ICQ		CyberNotes 2000-20
Trojan/Parkinson		CyberNotes 2000-21
Trojan/PSW.StealthD		CyberNotes 2000-19
Trojan/Ring0.B		CyberNotes 2000-24
Trojan/Twinshoe		CyberNotes 2000-24
Trojan/Varo31		CyberNotes 2000-19
Trojan/Win32		CyberNotes 2000-21
TryIt		CyberNotes 2000-05
VBS_MAILPEEP		CyberNotes 2000-22
W32.Nuker.C		CyberNotes 2000-14
wCrat	v1.2b	CyberNotes 2000-05
Win.Unabomber		CyberNotes 2000-14
WinCrash	Beta	CyberNotes 2000-12
Winkiller		CyberNotes 2000-12

-
- 1 L0pht Advisory, May 18, 2000.
 - 2 Securiteam, June 9, 2000.
 - 3 Securiteam, October 5, 2000.
 - 4 Bugtraq, November 20, 2000.
 - 5 Shadow Penguin Security, SPS Advisory #39, July 26, 2000.
 - 6 Bugtraq, April 20, 2000.
 - 7 Bugtraq, July 11, 2000.
 - 8 Bugtraq, September 24, 2000.
 - 9 Securiteam, November 29, 2000.
 - 10 L0pht Research Labs Security Advisory, May 4, 2000.
 - 11 NSFOCUS Security Advisory, SA2000-09, December 13, 2000.
 - 12 Bugtraq, February 27, 2000.
 - 13 FreeBSD Security Advisory, FreeBSD-SA-00:16, May 9, 2000.
 - 14 Allaire Security Bulletin, ASB00-12, May 8, 2000.
 - 15 Securiteam, May 13, 2000.
 - 16 Foundstone Advisory, June 7, 2000.
 - 17 Bugtraq, March 5, 2000.
 - 18 Allaire Security Bulletin, ASB00-03, January 4, 2000.
 - 19 Bugtraq, December 8, 2000.
 - 20 Allaire Secure Advisory, ASB00-06, April 3, 2000.
 - 21 Allaire Security Bulletin, ASB00-28, October 24, 2000.
 - 22 Allaire Security Bulletin, ASB00-29, October 23, 2000.
 - 23 Allaire Security Bulletin, ASB00-27, October 23, 2000.
 - 24 Allaire Security Bulletin, ASB00-02, January 4, 2000.
 - 25 Securiteam, February 1, 2000.
 - 26 Allaire Security Bulletin, ASB00-01, January 4, 2000.
 - 27 Allaire Security Bulletin, ASB00-23, August 30, 2000.
 - 28 Securiteam, June 9, 2000.
 - 29 USSR Labs, USSR-99029, December 31, 1999.
 - 30 NTBugtraq, August 9, 2000.
 - 31 Bugtraq, December 13, 2000.
 - 32 Infosec Security Vulnerability Report, Infosec.20000712, July 12, 2000.
 - 33 VIGILANTE Security Advisory, VIGILANTE-2000012, September 18, 2000.
 - 34 SuSE Security Announcement, July 10, 2000.
 - 35 Bugtraq, October 3, 2000.
 - 36 Securiteam, May 15, 2000.
 - 37 Securiteam, March 7, 2000.
 - 38 Para-Sentinel Report, 2000-04, January 25, 2000.
 - 39 Securiteam, December 29, 1999.
 - 40 Foundstone, Inc. Security Advisory, FS-072500-7-ANA, July 25, 2000.
 - 41 USSR Labs Advisory, USSR-20000045, June 15, 2000.
 - 42 Foundstone, Inc. Security Advisory, FS-072600-8-ANA, July 26, 2000.
 - 43 Bugtraq, March 25, 2000.
 - 44 Securiteam, October 3, 2000.
 - 45 Securiteam, June 8, 2000.
 - 46 CHINANSL Security Advisory, CSA-200011, December 6, 2000.
 - 47 Bugtraq, May 2, 2000.
 - 48 John A. Copeland, Professor, Georgia Tech ECE, December 29, 1999.
 - 49 Bugtraq, December 31, 1999.
 - 50 Securiteam, August 22, 2000.
 - 51 Bugtraq, November 19, 2000.
 - 52 USSR Advisory Code, USSR-2000039, May 1, 2000.
 - 53 Securiteam, April 27, 2000.
 - 54 USSR Labs Advisory Code, USSR-200035, March 15, 2000.
 - 55 USSR Labs Advisory Code, USSR-200036, March 16, 2000.

-
- 56 NTBugtraq, January 18, 2000.
 - 57 USSR Labs, USSR-99025, December 27, 1999.
 - 58 Bugtraq, October 24, 2000.
 - 59 NTSecurity, April 19, 2000.
 - 60 Securiteam, February 3, 2000.
 - 61 RFP2K05, May 18, 2000.
 - 62 Infosec Security Vulnerability Report No: Infosec.20000207.axis700.a, February 7, 2000.
 - 63 Infosec Security Vulnerability Report, February 29, 2000.
 - 64 MDMA Crew, July 30, 2000.
 - 65 BalaBit Security Advisory, BB-2000/01, November 22, 2000.
 - 66 Securiteam, October 16, 2000.
 - 67 SecurityFocus, October 27, 2000.
 - 68 Bugtraq, July 11, 2000.
 - 69 Bugtraq, October 10, 2000.
 - 70 Bugtraq, April 10, 2000.
 - 71 Foundstone, Inc. Security Advisory, FS-072800-9-BEA, July 28, 2000.
 - 72 Foundstone, Inc. Security Advisory, FS-073100-10-BEA, July 31, 2000.
 - 73 Foundstone, Inc. Security Advisory, FS-062100-4-BEA, June 21, 2000.
 - 74 BEA Systems Inc. Security Advisory, BEA00-05.01, August 14, 2000.
 - 75 eSecurityOnline.com Free Vulnerability Alert 3145, November 15, 2000.
 - 76 TESO Security Advisory, 2000/03/30, April 1, 2000.
 - 77 UssrLabs, November 24, 1999.
 - 78 Labs Advisory Code: RLA002, February 29, 2000.
 - 79 NTSecurity, July 10, 2000.
 - 80 Bugtraq, July 18, 2000.
 - 81 Securiteam, September 14, 2000.
 - 82 Bugtraq, April 10, 2000.
 - 83 s0ftpr0ject Advisory, SPIJ-003-000, May 2, 2000.
 - 84 Securiteam, September 11, 2000.
 - 85 USSR Labs Advisory, USSR-99028, December 30, 1999.
 - 86 Securiteam, December 10, 2000.
 - 87 Securiteam, November 28, 2000.
 - 88 Securiteam, February 10, 2000.
 - 89 Bugtraq, October 8, 2000.
 - 90 Bugtraq, March 4, 2000.
 - 91 Caldera Systems, Inc. Security Advisory, CSSA-2000-002.0, February 3, 2000.
 - 92 Caldera Security Advisory, June 2, 2000.
 - 93 Bugtraq, June 6, 2000.
 - 94 Securiteam, June 6, 2000.
 - 95 Red Hat, Inc. Security Advisory, RHSA-2000:094-01, October 26, 2000.
 - 96 Securax-SA-09 Security Advisory, December 5, 2000.
 - 97 eSecurityOnline.com, Vulnerability Alert 3092, November 2, 2000.
 - 98 eSecurityOnline.com Free Vulnerability Alert 3182, November 28, 2000.
 - 99 Bugtraq, May 25, 2000.
 - 100 Bugtraq, May 5, 2000.
 - 101 Bugtraq, May 23, 2000.
 - 102 Bugtraq, August 23, 2000.
 - 103 Bugtraq, August 30, 2000.
 - 104 Bugtraq, August 30, 2000.
 - 105 eSecurityOnline.com, October 18, 2000.
 - 106 Securiteam, October 30, 2000.
 - 107 Bugtraq, August 23, 2000.
 - 108 Bugtraq, December 12, 2000.
 - 109 eSecurityOnline.com Free Vulnerability Alert 3099, November 2, 2000.
 - 110 Bugtraq, July 4, 2000.

-
- ¹¹¹ Bugtraq, November 1, 2000.
¹¹² Check Point Software, June 7, 2000.
¹¹³ Bugtraq, March 14, 2000.
¹¹⁴ Securiteam, July 10, 2000.
¹¹⁵ Securiteam, August 7, 2000.
¹¹⁶ SecurityFocus, February 9, 2000.
¹¹⁷ SecureXpert Labs Advisory, SX-20000620-3, June 30, 2000.
¹¹⁸ Securiteam, January 24, 2000.
¹¹⁹ Securiteam, January 30, 2000.
¹²⁰ eSecurityOnline.com Free Vulnerability Alert 3186, November 29, 2000.
¹²¹ Cisco Advisory, CI-00.11, December 6, 2000.
¹²² Cisco Security Advisory, CI-00.02, April 19, 2000.
¹²³ Defcom Labs Advisory, def-2000-02, October 26, 2000.
¹²⁴ Bugtraq, October 22, 2000.
¹²⁵ Cisco Security Advisory, CI-00.06, August 2, 2000.
¹²⁶ Cisco Security Advisory, CI-00.09, October 25, 2000.
¹²⁷ Securiteam, November 30, 2000.
¹²⁸ Bugtraq, May 2, 2000.
¹²⁹ Cisco Security Advisory, July 11, 2000.
¹³⁰ Cisco Security Advisory, September 21, 2000.
¹³¹ Cisco Field Notice, March 16, 2000.
¹³² Solar Designer, May 30, 2000.
¹³³ @stake, Inc. Security Advisory, A102600-1, October 26, 2000.
¹³⁴ Securiteam, Mar 2, 2000.
¹³⁵ Securiteam, May 17, 2000.
¹³⁶ Cisco Security Advisory, CI-00.03, April 19, 2000.
¹³⁷ Vnunet.com, June 6, 2000.
¹³⁸ Bugtraq, September 19, 2000.
¹³⁹ Securiteam, October 9, 2000.
¹⁴⁰ Bugtraq, March 29, 2000.
¹⁴¹ Delphis Internet Consulting Security Team, June 6, 2000.
¹⁴² Securiteam, April 10, 2000.
¹⁴³ Chris Adams, May 23, 2000.
¹⁴⁴ Cobalt Networks Security Advisory, 03.31.2000, March 31 2000.
¹⁴⁵ Cobalt Networks Security Advisory, 01.31.2000, January 31, 2000.
¹⁴⁶ iXsecurity Security Vulnerability Report, 20001107, November 7, 2000.
¹⁴⁷ Bugtraq, July 28, 2000.
¹⁴⁸ Bugtraq, August 11, 2000.
¹⁴⁹ Bugtraq, November 10, 2000.
¹⁵⁰ Securiteam, June 15, 2000.
¹⁵¹ Bugtraq, January 18, 2000.
¹⁵² Delphis Internet Consulting Security Team, June 8, 2000.
¹⁵³ Bugtraq, July 29, 2000.
¹⁵⁴ Conectiva Linux Security Announcement, 2000-07-26:ldap, July 26, 2000.
¹⁵⁵ Securiteam, February 26, 2000.
¹⁵⁶ Bugtraq, January 14, 2000.
¹⁵⁷ Bugtraq, March 3, 2000.
¹⁵⁸ L0pht Research Labs Security Advisory, April 10, 2000.
¹⁵⁹ Bugtraq, November 2, 2000.
¹⁶⁰ USSR Labs, USSR-99027, December 29, 1999.
¹⁶¹ Securiteam, July 20, 2000.
¹⁶² Bugtraq, January 12, 2000.
¹⁶³ Bugtraq, July 3, 2000.
¹⁶⁴ SecurityFocus, June 28, 2000.
¹⁶⁵ Bugtraq, February 3, 2000.

-
- ¹⁶⁶Debian Security Advisory, Debian-00-33-1, October 14, 2000.
- ¹⁶⁷Bugtraq, April 11, 2000.
- ¹⁶⁸b0f-SA2000-002, April 12, 2000.
- ¹⁶⁹Bugtraq, October 3, 2000.
- ¹⁷⁰Securiteam, September 1, 2000.
- ¹⁷¹Cgi Security Advisory #2, November 14, 2000.
- ¹⁷²Debian Security Advisory, October 9, 2000.
- ¹⁷³Securiteam, June 22, 2000.
- ¹⁷⁴Debian Security Advisory, February 20, 2000.
- ¹⁷⁵SecurityFocus, February 2, 2000.
- ¹⁷⁶Debian Security Advisory, February 1, 2000.
- ¹⁷⁷Debian Security Advisory, 00-005, March 1, 2000.
- ¹⁷⁸RHSA-2000:006-01, March 6, 2000.
- ¹⁷⁹Bugtraq, June 5, 2000.
- ¹⁸⁰Securiteam, June 20, 2000.
- ¹⁸¹SecurityFocus, February 20, 2000.
- ¹⁸²Blue Panda Vulnerability Announcement, August 4, 2000.
- ¹⁸³Bugtraq, May 24, 2000.
- ¹⁸⁴USSR Labs, USSR-2000032, February 4, 2000.
- ¹⁸⁵Enigma Security Advisory, September 19, 2000.
- ¹⁸⁶Securiteam, March 6, 2000.
- ¹⁸⁷14x Network Security Inc., May 22, 2000.
- ¹⁸⁸USSR Advisory Code, USSR-2000052, August 31, 2000.
- ¹⁸⁹Securiteam, October 25, 2000.
- ¹⁹⁰Secure Reality Pty Ltd. Security Advisory , SRADV00005, December 6, 2000.
- ¹⁹¹Bugtraq, June 6, 2000.
- ¹⁹²MDMA Advisory #6, June 6, 2000.
- ¹⁹³Bugtraq, October 9, 2000.
- ¹⁹⁴Bugtraq, September 21, 2000.
- ¹⁹⁵Bugtraq, October 9, 2000.
- ¹⁹⁶Delphis Consulting Plc Security Team Advisories, DST2K0027, September 12, 2000.
- ¹⁹⁷Delphis Consulting Plc Security Team Advisories, DST2K0028, September 12, 2000.
- ¹⁹⁸USSR Labs, USSR Advisory Code 22, December 21, 1999.
- ¹⁹⁹SecurityFocus, May 2, 2000.
- ²⁰⁰Authentix Security Advisory, Authentix100, November 1, 2000.
- ²⁰¹Bugtraq, June 26, 2000.
- ²⁰²Bugtraq, June 27, 2000.
- ²⁰³Securiteam, June 29, 2000.
- ²⁰⁴Bugtraq, November 11, 2000.
- ²⁰⁵Bugtraq, February 28, 2000.
- ²⁰⁶Bugtraq, March 13, 2000.
- ²⁰⁷Securiteam, August 21, 2000.
- ²⁰⁸FreeBSD Security Advisory, June 7, 2000.
- ²⁰⁹FreeBSD Security Advisory, SA-00:04, February 19, 2000.
- ²¹⁰FreeBSD Security Advisory, FreeBSD-SA-00:42, August 28, 2000.
- ²¹¹FreeBSD Security Advisory, FreeBSD-SA-00:41, August 28, 2000.
- ²¹²FreeBSD Ports Security Advisory, FreeBSD-SA-00:49, September 13, 2000.
- ²¹³FreeBSD Security Advisory, FreeBSD-SA-00:69, November 15, 2000.
- ²¹⁴FreeBSD Security Advisory, FreeBSD-SA-00:24, July 6, 2000.
- ²¹⁵Bugtraq, October 21, 2000.
- ²¹⁶SecurityFocus. January 21, 2000.
- ²¹⁷FreeBSD, Inc. Security Advisory, FreeBSD-SA-00:52, October 6, 2000.
- ²¹⁸FreeBSD Security Advisory, SA-00:03, February 19, 2000.
- ²¹⁹Securiteam, December 17, 1999.
- ²²⁰Buffer Overflow Security Advisory # 3, April 24, 2000.

-
- ²²¹FreeBSD Security Advisory, SA-00:01, January 19, 2000.
- ²²²FreeBSD Security Advisory, FreeBSD-SA-00:70, November 14, 2000.
- ²²³FreeBSD Security Advisory, FreeBSD-SA-00:43, August 28, 2000.
- ²²⁴FreeBSD Ports Security Advisory, FreeBSD-SA-00:66, November 6, 2000.
- ²²⁵Securiteam, May 19, 2000.
- ²²⁶FreeBSD Security Advisory, FreeBSD-SA-00:63, November 2, 2000.
- ²²⁷FreeBSD Security Advisory, FreeBSD-SA-00:54, October 13, 2000.
- ²²⁸FreeBSD Security Advisory, SA-00:10, March 16, 2000.
- ²²⁹FreeBSD-SA-00:13, April 19, 2000.
- ²³⁰FreeBSD Ports Security Advisory, FreeBSD-SA-00:64, November 6, 2000.
- ²³¹FreeBSD Security Advisory, June 12, 2000.
- ²³²FreeBSD Security Advisory, FreeBSD-SA-00:36, August 14, 2000.
- ²³³FreeBSD Security Advisory, FreeBSD-SA-00:40, August 28, 2000.
- ²³⁴FreeBSD Security Advisory, SA-00:05, February 28, 2000.
- ²³⁵FreeBSD Ports Security Advisory, FreeBSD-SA-00:47, September 13, 2000.
- ²³⁶FreeBSD Ports Security Advisory, FreeBSD-SA-00:26, July 11, 2000.
- ²³⁷FreeBSD Security Advisory, June 7, 2000.
- ²³⁸FreeBSD-SA-00:12, April 10, 2000.
- ²³⁹FreeBSD Security Advisory, FreeBSD-SA-00:62, November 1, 2000.
- ²⁴⁰FreeBSD Security Advisory, FreeBSD-SA-00:62, Reissued November 6, 2000.
- ²⁴¹FreeBSD Security Advisory: FreeBSD-SA-00:02.procfs, January 28, 2000.
- ²⁴²Bugtraq, December 27, 1999.
- ²⁴³SecurityFocus, February 25, 2000.
- ²⁴⁴Securiteam, July 17, 2000.
- ²⁴⁵Security Alert Consensus Number 038 (00.14), March 30, 2000.
- ²⁴⁶Securiteam, May 17, 2000.
- ²⁴⁷Bugtraq, June 26, 2000.
- ²⁴⁸Bugtraq, January 5, 2000.
- ²⁴⁹Bugtraq, August 31, 2000.
- ²⁵⁰Bugtraq, September 26, 2000.
- ²⁵¹Bugtraq, October 2, 2000.
- ²⁵²Bugtraq, September 7, 2000.
- ²⁵³Debian Security Advisory, Debian-00-015, July 28, 2000.
- ²⁵⁴Bugtraq, October 13, 2000.
- ²⁵⁵Securiteam, August 28, 2000.
- ²⁵⁶VIGILANTE Advisory Code, VIGILANTE-2000008, September 4, 2000.
- ²⁵⁷Bugtraq, December 1, 2000.
- ²⁵⁸Securiteam, December 29, 1999.
- ²⁵⁹Securiteam, November 11, 2000.
- ²⁶⁰Bugtraq, August 29, 2000.
- ²⁶¹Securiteam, February 3, 2000.
- ²⁶²SecurityFocus, January 6, 2000.
- ²⁶³Helix Code, Inc. Security Advisory, 08-20-2000-02, August 20, 2000.
- ²⁶⁴Helix Code, Inc. Security Advisory, August 29, 2000.
- ²⁶⁵HP-UX Security Advisory, HPSBUX0011-131, November 21, 2000.
- ²⁶⁶USSR Labs, May 24, 2000.
- ²⁶⁷USSR Labs, May 24, 2000.
- ²⁶⁸Delphis Internet Consulting Security Team, June 8, 2000.
- ²⁶⁹Hewlett-Packard Security Advisory, 00111, February 17, 2000.
- ²⁷⁰Hewlett-Packard Security Advisory, HPSBUX0011-128, November 2, 2000.
- ²⁷¹Bugtraq, November 2, 2000.
- ²⁷²Hewlett-Packard Company Security Bulletin, HPSBUX0011-130, November 13, 2000.
- ²⁷³Bugtraq, November 8, 2000.
- ²⁷⁴Delphis Internet Consulting Security Team, June 8, 2000.
- ²⁷⁵Daily Security Bulletins Digest, HPSBUX9910-104, May 3, 2000.

-
- ²⁷⁶ eSecurityOnline.com Vulnerability Alert 3071, October 24, 2000.
- ²⁷⁷ Bugtraq, July 27, 2000.
- ²⁷⁸ Hewlett-Packard Company Security Bulletin, HPSBUX0008-118, August 9, 2000.
- ²⁷⁹ Hewlett-Packard Security Bulletin, HPSBUX0011-129, November 8, 2000.
- ²⁸⁰ Hewlett-Packard Security Advisory, HPSBUX0004-112, April 4, 2000.
- ²⁸¹ VIGILANTE-2000004, July 19, 2000.
- ²⁸² Bugtraq, April 20, 2000.
- ²⁸³ VIGILANTE Security Advisory, VIGILANTE-2000014, October 10, 2000.
- ²⁸⁴ Hewlett-Packard Advisory, 0007, 26 June 2000.
- ²⁸⁵ Hewlett-Packard Company Security Bulletin, HPSBUX0009-122, September 27, 2000.
- ²⁸⁶ Hewlett-Packard Company Security Bulletin, HPSBUX0009-120, September 13, 2000.
- ²⁸⁷ Hewlett-Packard Company Security Bulletin, HPSBUX0008-119, August 9, 2000.
- ²⁸⁸ Hewlett-Packard Daily Security Bulletins Digest, #00121, September 25, 2000.
- ²⁸⁹ Bugtraq, February 28, 2000.
- ²⁹⁰ Bugtraq, June 7, 2000.
- ²⁹¹ SecurityFocus, October 27, 2000.
- ²⁹² HP Security Advisory #00109, January 6, 2000.
- ²⁹³ Hewlett-Packard Security Advisory, HPSBUX9912-106, December 13, 1999.
- ²⁹⁴ Hewlett-Packard Security Advisory, HPSBUX9912-106, revised January 17, 2000.
- ²⁹⁵ Hewlett-Packard Security Advisory, HPSBUX0001-110, January 24, 2000.
- ²⁹⁶ Network Computing Security Express #032, February 17, 2000.
- ²⁹⁷ SecurityFocus, December 31, 1999.
- ²⁹⁸ Securiteam, September 12, 2000.
- ²⁹⁹ Secure Reality Pty Ltd. Security Advisory #3, SRADV00003, September 12, 2000.
- ³⁰⁰ SecurityFocus, December 27, 1999.
- ³⁰¹ Securiteam, November 3, 2000.
- ³⁰² Securiteam, December 4, 2000.
- ³⁰³ Bugtraq, March 14, 2000.
- ³⁰⁴ Securiteam, June 22, 2000.
- ³⁰⁵ ISS Security Advisory, April 26, 2000.
- ³⁰⁶ eSecurityOnline.com Free Vulnerability Alert 3225, December 14, 2000.
- ³⁰⁷ Securiteam, December 14, 2000.
- ³⁰⁸ Bugtraq, November 23, 2000.
- ³⁰⁹ Bugtraq, April 5, 2000.
- ³¹⁰ Securiteam, May 27, 2000.
- ³¹¹ Securiteam, May 27, 2000.
- ³¹² Bugtraq, November 28, 2000.
- ³¹³ Internet Security Systems Security Advisory, September 7, 2000.
- ³¹⁴ Technotronic, December 27, 1999.
- ³¹⁵ Vigilante Security Advisory, VIGILANTE-2000006, August 15, 2000.
- ³¹⁶ Foundstone, Inc. Security Advisory, FS-072400-6-IBM, July 23, 2000.
- ³¹⁷ Securiteam, September 20, 2000.
- ³¹⁸ Securiteam, June 2, 2000.
- ³¹⁹ Securiteam, June 7, 2000.
- ³²⁰ Securiteam, May 2, 2000.
- ³²¹ Internet Security Systems Security Advisory, May 3, 2000.
- ³²² ISSAlert, June 7, 2000.
- ³²³ SecurityFocus, March 29, 2000.
- ³²⁴ BluePanda Vulnerability Announcement, June 26, 2000.
- ³²⁵ Crimelabs Security Advisory, CLABS200003, April 24, 2000.
- ³²⁶ Securiteam, April 11, 2000.
- ³²⁷ Bugtraq, February 13, 2000.
- ³²⁸ Securiteam, July 18, 2000.
- ³²⁹ Securiteam, December 13, 2000.
- ³³⁰ USSR Advisory Code, USSR-2000056, October 30, 2000.

-
- ³³¹ VIGILANTE Advisory Code, VIGILANTE- 2000010, September 6, 2000.
- ³³² VIGILANTE Advisory Code, VIGILANTE-2000007, August 28, 2000.
- ³³³ SecurityFocus, January 4, 2000.
- ³³⁴ Securiteam, October 21, 2000.
- ³³⁵ L0pht Research Labs Security Advisory, May 8, 2000.
- ³³⁶ Bugtraq, June 29, 2000.
- ³³⁷ SecurityFocus, January 21, 2000.
- ³³⁸ Delphis Consulting Plc Security Team Advisories, DST2K0018, June 19, 2000.
- ³³⁹ Securiteam, July 5, 2000.
- ³⁴⁰ Bugtraq, February 29, 2000.
- ³⁴¹ Securiteam, August 23, 2000.
- ³⁴² TESO Security Advisory, February 11, 2000.
- ³⁴³ Securiteam, February 26, 2000.
- ³⁴⁴ SecurityFocus, December 22, 1999.
- ³⁴⁵ NTBugtraq, August 17, 2000.
- ³⁴⁶ Bugtraq, August 30, 2000.
- ³⁴⁷ USSRLabs, USSR Advisory Code: USSR-2000-30 January 5, 2000.
- ³⁴⁸ Bugtraq, April 5, 2000.
- ³⁴⁹ Bugtraq, December 7, 2000.
- ³⁵⁰ VIGILANTE Security Advisory, VIGILANTE-200001, September 19, 2000.
- ³⁵¹ Securiteam, July 17, 2000.
- ³⁵² Delphis Internet Consulting Security Team, June 9, 2000.
- ³⁵³ Delphis Consulting Plc Security Team Advisories, DST2K0007, May 30, 2000.
- ³⁵⁴ Securiteam, September 13, 2000.
- ³⁵⁵ Securiteam, September 15, 2000.
- ³⁵⁶ Bugtraq, July 11, 2000.
- ³⁵⁷ Bugtraq, September 19, 2000.
- ³⁵⁸ Bugtraq, May 17, 2000.
- ³⁵⁹ SuSE Security Announcement, May 29, 2000.
- ³⁶⁰ Bugtraq, November 26, 2000.
- ³⁶¹ Strumpf Noir Society Advisories, December 7, 2000.
- ³⁶² eSecurityOnline.com Vulnerability Alert 2984, September 19, 2000.
- ³⁶³ Bugtraq, August, 5, 2000.
- ³⁶⁴ Bugtraq, October 29, 2000.
- ³⁶⁵ eSecurityOnline.com, October 17, 2000.
- ³⁶⁶ Bugtraq, December 8, 2000.
- ³⁶⁷ Bugtraq, May 2, 2000.
- ³⁶⁸ FreeBSD Security Advisory, FreeBSD-SA-00:61, October 30, 2000.
- ³⁶⁹ Updated FreeBSD Security Advisory, FreeBSD-SA-00:61, November 6, 2000.
- ³⁷⁰ Bugtraq, December 11, 2000.
- ³⁷¹ Bugtraq, December 14, 2000.
- ³⁷² Bugtraq, December 11, 2000.
- ³⁷³ Bugtraq, August 3, 2000.
- ³⁷⁴ Delphis Internet Consulting Security Team, June 8, 2000.
- ³⁷⁵ TESO Security Advisory, 09/03/2000, March 11, 2000.
- ³⁷⁶ Bugtraq, December 21, 1999.
- ³⁷⁷ S.A.F.E.R. Security Bulletin, 001103.EXP.1.9, November 3, 2000.
- ³⁷⁸ Securiteam, November 10, 2000.
- ³⁷⁹ Securiteam, November 26, 2000.
- ³⁸⁰ Bugtraq, December 21, 1999.
- ³⁸¹ Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2000-07, July 17, 2000.
- ³⁸² Linux-Mandrake Security Update Advisory, MDKSA-2000:034, August 12, 2000.
- ³⁸³ Linux-Mandrake Security Update Advisory, MDKSA-2000:052, October 2, 2000.
- ³⁸⁴ Linux-Mandrake Security Update Advisory, MDKSA-2000:046, September 11, 2000.
- ³⁸⁵ Bugtraq, March 9, 2000.

³⁸⁶Bugtraq, May 26, 2000.
³⁸⁷Linux-Mandrake Security Update Advisory, MDKSA-2000:020, July 18, 2000.
³⁸⁸Bugtraq, May 27, 2000.
³⁸⁹MandrakeSoft, June 5, 2000.
³⁹⁰Bugtraq, February 28, 2000.
³⁹¹Bugtraq, November 20, 2000.
³⁹²Bugtraq, May 22, 2000.
³⁹³Perfecto's Black Watch Labs Advisory, BWL 00-06, May 10, 2000.
³⁹⁴Bugtraq, May 16, 2000.
³⁹⁵Securiteam, November 15, 2000.
³⁹⁶NTBugtraq, November 3, 2000.
³⁹⁷Cerberus Information Security Advisory, CISADV000427, April 27, 2000.
³⁹⁸bunny69, May 22, 2000.
³⁹⁹Xato Network Security Advisory, XATO-112000-01, November 9, 2000.
⁴⁰⁰Bugtraq, January 5, 2000.
⁴⁰¹Bugtraq, February 1, 2000.
⁴⁰²DeepZone Advisory, August 10, 2000.
⁴⁰³Securiteam, October 14, 2000.
⁴⁰⁴Bugtraq, December 7, 2000.
⁴⁰⁵Bugtraq, May 22, 2000.
⁴⁰⁶Bugtraq, March 31, 2000.
⁴⁰⁷Bugtraq, February 1, 2000.
⁴⁰⁸Georgi Guninski Security Advisory #17, August 7, 2000.
⁴⁰⁹Microsoft Security Bulletin, MS00-034, May 12, 2000.
⁴¹⁰Bugtraq, May 13, 2000.
⁴¹¹Microsoft Security Bulletin, MS00-015, March 7, 2000.
⁴¹²Microsoft Security Advisory, MS00-019, March 30, 2000.
⁴¹³Microsoft Security Bulletin, MS00-002, January 21, 2000.
⁴¹⁴Microsoft Security Bulletin, MS00-092, December 1, 2000.
⁴¹⁵ISS Security Advisory, March 14, 2000.
⁴¹⁶Microsoft Security Bulletin, MS00-056, August 10, 2000.
⁴¹⁷Microsoft Security Bulletin, MS00-022, April 3, 2000
⁴¹⁸Microsoft Security Bulletin, MS00-088, November 16, 2000.
⁴¹⁹Securiteam, April 20, 2000.
⁴²⁰Securiteam, August 24, 2000.
⁴²¹Bugtraq, July 4, 2000.
⁴²²Cerberus Information Security Advisory (CISADV000203), February 3, 2000.
⁴²³Bugtraq, February 16, 2000.
⁴²⁴Bugtraq, January 3, 2000.
⁴²⁵Securiteam, May 11, 2000.
⁴²⁶SecurityFocus, February 9, 2000.
⁴²⁷Cerberus Information Security Advisory, CISADV000330, March 31, 2000.
⁴²⁸Microsoft Security Bulletin, MS00-084, November 2, 2000.
⁴²⁹Georgi Guninski Security Advisory #27, November 10, 2000.
⁴³⁰Microsoft Security Bulletin, MS00-033, May 17, 2000.
⁴³¹Microsoft Security Bulletin, MS00-009, February 16, 2000.
⁴³²Microsoft Security Bulletin, MS00-042, June 29, 2000.
⁴³³NTBugtraq, June 6, 2000.
⁴³⁴Microsoft Security Bulletin, MS00-033, May 17, 2000.
⁴³⁵Microsoft Security Bulletin, MS00-033, May 17, 2000.
⁴³⁶ACROS Penetration Team, June 5, 2000.
⁴³⁷Microsoft Security Bulletin, MS99-060, December 22, 1999.
⁴³⁸Microsoft Security Bulletin, MS00-055, August 9, 2000.
⁴³⁹Microsoft Security Bulletin, MS00-076, October 12, 2000.
⁴⁴⁰NTSecurity, March 10, 2000.

441 Securiteam, March 3, 2000.
442 Securiteam, June 27, 2000.
443 Bugtraq, December 22, 1999.
444 Georgi Guninski Security Advisory #20, September 4, 2000.
445 Georgi Guninski Security Advisory #16, July 14, 2000.
446 Georgi Guninski Security Advisory #14, June 27, 2000.
447 Georgi Guninski Security Advisory #29, 2000, November 23, 2000.
448 Securiteam, April 18, 2000.
449 Microsoft Security Bulletin, MS00-093, December 1, 2000.
450 Security Alert Consensus #054, July 20, 2000.
451 Microsoft Security Bulletin, MS00-018, March 21, 2000.
452 Microsoft Security Bulletin, MS00-023, April 12, 2000.
453 Microsoft Security Bulletin, MS00-031, May 10, 2000.
454 Microsoft Security Bulletin, MS00-030, May 12, 2000.
455 Microsoft Security Bulletin, MS00-044, July 14, 2000.
456 Microsoft Security Bulletin, MS00-057, August 10, 2000.
457 Securiteam, May 16, 2000.
458 Microsoft Security Bulletin, MS00-058, August 14, 2000.
459 @stake, Inc., A100400-1, October 4, 2000.
460 Bugtraq, January 20, 2000.
461 Bugtraq, November 3, 2000.
462 Microsoft Security Bulletin, MS00-078, October 17, 2000.
463 Microsoft Security Bulletin, MS00-080, October 23, 2000.
464 Microsoft Security Bulletin, MS00-063, September 5, 2000.
465 Microsoft Security Bulletin, MS99-061, December 21, 1999.
466 Microsoft Security Bulletin, MS99-058, December 21, 1999.
467 Microsoft Security Bulletin, MS00-090, November 22, 2000.
468 Microsoft Security Bulletin, MS00-001, January 4, 2000.
469 Microsoft Security Bulletin, MS00-082, October 31, 2000.
470 NSFOCUS Security Advisory, SA2000-08, December 13, 2000.
471 Georgi Guninski Security Advisory #21, September 18, 2000.
472 Microsoft Security Bulletin, MS00-085, November 2, 2000.
473 Microsoft Security Bulletin, MS00-061, August 25, 2000.
474 Microsoft Security Bulletin, MS00-077, October 13, 2000.
475 Microsoft Security Bulletin, MS00-052, July 28, 2000.
476 George Guninski Security Advisory #9, March 14, 2000.
477 Securiteam, June 12, 2000.
478 Bugtraq, August 25, 2000.
479 Weekly Microsoft Security Roundup, March 2-3, 2000.
480 Securiteam, September 1, 2000.
481 Securiteam, May 13, 2000.
482 Microsoft Security Bulletin, MS00-045, July 20, 2000.
483 Microsoft Security Bulletin, MS00-046, July 20, 2000.
484 Microsoft Security Bulletin, MS00-043, July 20, 2000.
485 Bugtraq, February 19, 2000.
486 Bugtraq, February 1, 2000.
487 Georgi Guninski Security Advisory #22, September 26, 2000.
488 Microsoft Security Bulletin, MS00-010, February 18, 2000.
489 ISSalert, May 9, 2000.
490 Microsoft Security Bulletin, MS99-049, December 20, 1999.
491 Microsoft Security Bulletin, MS00-048, July 7, 2000.
492 Microsoft Security Bulletin, MS00-035, May 30, 2000.
493 Microsoft Security Bulletin, MS00-014, March 8, 2000.
494 Microsoft Security Bulletin, MS00-012, February 22, 2000.
495 Microsoft Security Bulletin, MS00-025, April 17, 2000.

⁴⁹⁶Bugtraq, February 15, 2000.
⁴⁹⁷Securiteam, March 3, 2000.
⁴⁹⁸Microsoft Security Bulletin, MS00-065, September 7, 2000.
⁴⁹⁹Microsoft Security Bulletin, MS00-062, August 28, 2000.
⁵⁰⁰Microsoft Security Bulletin, MS00-020, June 15, 2000.
⁵⁰¹Internet Security Systems SAVANT Windows 2000 Advisory No, 00/26, May 10, 2000.
⁵⁰²Microsoft Security Bulletin, MS-0026, April 20, 2000.
⁵⁰³Bugtraq, June 29, 2000.
⁵⁰⁴Microsoft Security Bulletin, MS00-091, November 30, 2000.
⁵⁰⁵Microsoft Security Bulletin, MS00-054, August 3, 2000.
⁵⁰⁶Microsoft Security Bulletin, MS00-005, January 17, 2000.
⁵⁰⁷NSFOCUS Security Advisory, SA2000-03, October 11, 2000.
⁵⁰⁸Microsoft Security Bulletin, MS00-073, October 11, 2000.
⁵⁰⁹Microsoft Security Bulletin, MS00-072, October 10, 2000.
⁵¹⁰Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2000-10, August 29, 2000.
⁵¹¹el8.org advisory, May 2, 2000.
⁵¹²Microsoft Security Bulletin, MS00-029, May 19, 2000.
⁵¹³Microsoft Security Bulletin, MS00-036, May 26, 2000.
⁵¹⁴Bugtraq, February 18, 2000.
⁵¹⁵Microsoft Security Bulletin, MS00-079, October 18, 2000.
⁵¹⁶Georgi Guninski Security Advisory #18, August 14, 2000.
⁵¹⁷Bugtraq, August 31, 2000.
⁵¹⁸Microsoft Security Bulletin, MS00-038, May 31, 2000.
⁵¹⁹Microsoft Security Bulletin, MS00-016, March 20, 2000.
⁵²⁰Microsoft Security Bulletin, MS00-068, September 26, 2000.
⁵²¹Microsoft Security Bulletin, MS00-013, February 23, 2000.
⁵²²Microsoft Security Bulletin, MS00-064, September 6, 2000.
⁵²³NTBugtraq, February 7, 2000.
⁵²⁴Microsoft Security Bulletin, MS00-053, August 2, 2000.
⁵²⁵Microsoft Security Bulletin, MS00-066, September 11, 2000.
⁵²⁶Microsoft Security Bulletin, MS00-067, September 21, 2000.
⁵²⁷Microsoft Security Bulletin, MS00-069, September 29, 2000.
⁵²⁸Bugtraq, November 29, 2000.
⁵²⁹Microsoft Security Bulletin, MS00-020, June 15, 2000.
⁵³⁰Microsoft Security Bulletin, MS00-089, November 21, 2000.
⁵³¹SecureXpert Labs Advisory, SX-20000620-2, June 30, 2000.
⁵³²Microsoft Security Bulletin, MS00-083, November 1, 2000.
⁵³³Microsoft Security Bulletin, MS00-008, March 9, 2000.
⁵³⁴SecurityFocus, March 20, 2000.
⁵³⁵Bugtraq, October 23, 2000.
⁵³⁶Bugtraq, November 22, 2000.
⁵³⁷Microsoft Security Bulletin, MS00-094, December 5, 2000.
⁵³⁸Microsoft Security Bulletin, MS00-004, January 21, 2000.
⁵³⁹Microsoft Security Bulletin, MS00-003, January 12, 2000.
⁵⁴⁰Microsoft Security Bulletin, MS00-070, October 3, 2000.
⁵⁴¹Securiteam, June 9, 2000.
⁵⁴²Microsoft Security Bulletin, MS00-047, July 27, 2000.
⁵⁴³Bugtraq, July 26, 2000.
⁵⁴⁴Microsoft Security Advisory, MS00-021, March 30, 2000.
⁵⁴⁵Securiteam, February 21, 2000.
⁵⁴⁶Microsoft Security Bulletin, MS00-087, November 8, 2000.
⁵⁴⁷Microsoft Security Bulletin, MS00-024, April 13, 2000.
⁵⁴⁸Microsoft Security Bulletin, MS00-07, February 1, 2000.
⁵⁴⁹Microsoft Security Bulletin, MS00-071, October 5, 2000.
⁵⁵⁰Bugtraq, February 25, 2000.

551 Microsoft Security Bulletin, MS00-086, updated November 10, 2000.
552 Microsoft Security Bulletin, MS00-086, updated November 21, 2000.
553 Georgi Guninski Security Advisory #23, October 5, 2000
554 Securiteam, October 19, 2000.
555 Microsoft Security Bulletin, MS00-059, August 21, 2000.
556 Microsoft Security Bulletin, MS00-075, October 12, 2000.
557 Bugtraq, September 12, 2000.
558 Microsoft Security Bulletin, MS00-074, October 11, 2000.
559 SecurityFocus, March 4, 2000.
560 Microsoft Security Bulletin, MS00-017, March 16, 2000.
561 Microsoft Security Bulletin, MS00-095, December 6, 2000.
562 Microsoft Security Bulletin, MS00-096, December 6, 2000.
563 Microsoft Security Bulletin, MS00-060, August 25, 2000.
564 Microsoft Security Bulletin, MS00-060, Re-release, November 2, 2000.
565 Georgi Guninski Security Advisory #15, July 11, 2000.
566 Microsoft Security Bulletin, MS00-051, July 26, 2000.
567 Bugtraq, February 1, 2000.
568 Microsoft Security Bulletin, MS00-011, February 19, 2000.
569 Microsoft Security Bulletin, MS00-035, June 15, 2000.
570 Microsoft Security Bulletin, MS00-041, July 12, 2000.
571 Microsoft Security Bulletin, MS00-032, June 2, 2000.
572 Microsoft Security Bulletin, MS00-032, July 26, 2000.
573 SecureXpert Labs Advisory, SX-20000620-1, June 30, 2000.
574 Microsoft Security Bulletin, MS00-050, July 24, 2000.
575 Georgi Guninski Security Advisory #13, June 27, 2000.
576 Microsoft Security Bulletin, MS00-049, July 14, 2000.
577 Microsoft Security Bulletin, MS00-049, re-released August 9, 2000.
578 Microsoft Security Bulletin, MS00-006, January 26, 2000.
579 Microsoft Security Bulletin, MS00-006, February 11, 2000.
580 Georgi Guninski Security Advisory #24, October 18, 2000.
581 Microsoft Security Bulletin, MS00-081, October 25, 2000.
582 Bugtraq, June 10, 2000.
583 Bugtraq, November 22, 2000.
584 Bugtraq, November 28, 2000.
585 Computer Journal c't (German computer technology journal), January 12, 2000.
586 Securiteam, August 29, 2000.
587 MIT, June 9, 2000.
588 @stake Advisory, A090800-1, September 8, 2000.
589 Bugtraq, March 10, 2000.
590 Bugtraq, February 10, 2000.
591 Securiteam, March 15, 2000.
592 Bugtraq, March 22, 2000.
593 TESO Security Advisory, 2000/03/13, March
594 NWC/SANS SAC Newsletter, #037, March 23, 2000.
595 Securiteam, March 14, 2000.
596 Red Hat, Inc. Security Advisory, RHSA-2000:008-01, March 29, 2000.
597 FreeBSD Security Advisory, FreeBSD-SA-00:11, April 10, 2000.
598 Allaire Security Bulletin, ASB00-15, June 22, 2000.
599 Bugtraq, December 6, 2000.
600 Fate Research Labs, November 20, 2000.
601 Bugtraq, November 14, 2000.
602 Securiteam, July 6, 2000.
603 eSecurityOnline.com Free Vulnerability Alert 3188, November 29, 2000.
604 CORE SDI Advisory ID, CORE-090400, September 4, 2000.
605 Securiteam, June 24, 2000.

-
- ⁶⁰⁶Bugtraq, November 5, 2000.
- ⁶⁰⁷eSecurityOnline.com Free Vulnerability Alert 3227, December 14, 2000.
- ⁶⁰⁸CERT Advisory, CA-2000-13, July 10, 2000.
- ⁶⁰⁹Bugtraq, December 8, 2000.
- ⁶¹⁰eSecurityOnline.com, October 4, 2000.
- ⁶¹¹Securiteam, November 28, 2000.
- ⁶¹²Bugtraq, August 26, 2000.
- ⁶¹³RUS-CERT Advisory, 200004-01, April 18, 2000.
- ⁶¹⁴Perfecto's Black Watch Labs Advisory, BWL 00-05, May 5, 2000.
- ⁶¹⁵Bugtraq, September 29, 2000.
- ⁶¹⁶Bugtraq, November 2, 2000.
- ⁶¹⁷Packet Knights Advisory 001, December 11, 2000.
- ⁶¹⁸CERT Advisory, CA-2000-20, November 14, 2000.
- ⁶¹⁹Securiteam, November 21, 2000.
- ⁶²⁰Securiteam, December 7, 2000.
- ⁶²¹FreeBSD Security Advisory, FreeBSD-SA-00:18, May 9, 2000.
- ⁶²²Secure Reality Pty Ltd. Security Advisory, SRADV00006, December 6, 2000.
- ⁶²³Bugtraq, June 20, 2000.
- ⁶²⁴Bugtraq, June 19, 2000.
- ⁶²⁵Securiteam, April 24, 2000.
- ⁶²⁶Bugtraq, December 11, 2000.
- ⁶²⁷Secure Reality Pty Ltd. Security Advisory, SRADV00007, December 7, 2000.
- ⁶²⁸Bugtraq, March 30, 2000.
- ⁶²⁹Securiteam, March 24, 2000.
- ⁶³⁰Bugtraq, June 8, 2000.
- ⁶³¹Bugtraq, November 30, 2000.
- ⁶³²Cerberus Information Security Advisory, CISADV000503, May 3, 2000.
- ⁶³³eSecurityOnline.com, Vulnerability Alert 3079, October 27, 2000.
- ⁶³⁴Bugtraq, October 27, 2000.
- ⁶³⁵SecurityFocus, February 15, 2000.
- ⁶³⁶OpenBSD Security Advisory, October 4, 2000.
- ⁶³⁷eSecurityOnline.com, October 2, 2000.
- ⁶³⁸Securiteam, June 26, 2000.
- ⁶³⁹Bugtraq, October 6, 2000.
- ⁶⁴⁰@stake Advisory, A 101200-1, October 12, 2000.
- ⁶⁴¹Bugtraq, April 20, 2000.
- ⁶⁴²Bugtraq, April 18, 2000.
- ⁶⁴³Securiteam, September 17, 2000.
- ⁶⁴⁴CORE SDI ADVISORY, CORE-2000-10-26, October 26, 2000.
- ⁶⁴⁵Securiteam, November 9, 2000.
- ⁶⁴⁶Bugtraq, May 22, 2000.
- ⁶⁴⁷Securiteam, October 19, 2000.
- ⁶⁴⁸Bugtraq, November 12, 2000.
- ⁶⁴⁹Securiteam, November 22, 2000.
- ⁶⁵⁰TESO Security Advisory, March 9, 2000.
- ⁶⁵¹Securiteam, August 25, 2000.
- ⁶⁵²Securiteam, June 27, 2000.
- ⁶⁵³Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2000-06, May 29, 2000.
- ⁶⁵⁴Red Hat, Inc. Security Advisory, RHSA-2000:052-02, August 11, 2000.
- ⁶⁵⁵Debian Security Advisory, August 18, 2000.
- ⁶⁵⁶FreeBSD Ports Security Advisory, FreeBSD-SA-00:38, August 14, 2000.
- ⁶⁵⁷Conectiva Linux Security Announcement, August 15, 2000.
- ⁶⁵⁸RedHat Security Advisory, RHSA-2000:041-02, July 3, 2000.
- ⁶⁵⁹Linux-Mandrake Security Update Advisory, 2000-07-07, July 7, 2000.
- ⁶⁶⁰Caldera Systems, Inc. Security Advisory, CSSA-2000-021.0, July 6, 2000.

-
- ⁶⁶¹Conectiva Linux Security Announcement, 2000-07-28:pam, July 27, 2000.
- ⁶⁶²Red Hat, Inc. Security Advisory, RHSA-2000:044-02, July 21, 2000.
- ⁶⁶³Debian Security Advisory, August 16, 2000.
- ⁶⁶⁴Conectiva Linux Security Announcement, August 17, 2000.
- ⁶⁶⁵FreeBSD Security Advisory, FreeBSD-SA-00:31, July 5, 2000.
- ⁶⁶⁶Debian Security Advisory, July 2, 2000.
- ⁶⁶⁷FreeBSD Security Advisory, FreeBSD-SA-00:29, July 5, 2000.
- ⁶⁶⁸NetBSD Security Advisory 2000-010, July 10, 2000.
- ⁶⁶⁹FreeBSD Security Advisory, FreeBSD-SA-00:19, May 30, 2000.
- ⁶⁷⁰NetBSD Security Advisory, 2000-004, May 27, 2000.
- ⁶⁷¹Conectiva Linux Security Announcement, 2000-08-02, August 2, 2000.
- ⁶⁷²Red Hat, Inc. Security Advisory, RHSA-2000:030-03, August 3, 2000.
- ⁶⁷³Securiteam, October 1, 2000.
- ⁶⁷⁴Bugtraq, October 6, 2000.
- ⁶⁷⁵Red Hat, Inc. Security Advisory, RHSA-2000:049-02, August 8, 2000.
- ⁶⁷⁶Debian Security Advisory, August 7, 2000.
- ⁶⁷⁷Bugtraq, August 8, 2000.
- ⁶⁷⁸Red Hat, Inc. Security Advisory, RHSA-2000:050-01, August 8, 2000.
- ⁶⁷⁹RedHat Security Advisory, RHSA-2000:012, April 24, 2000.
- ⁶⁸⁰Mandrake Security Update, April 22, 2000.
- ⁶⁸¹TurboLinux Security Announcement, TLSA2000003-1, March 8, 2000.
- ⁶⁸²Bugtraq, March 3, 2000.
- ⁶⁸³Conectiva Linux Security Announcement, June 30, 2000.
- ⁶⁸⁴Linux-Mandrake Security Update Advisory, MDKSA-2000:018, July 11, 2000.
- ⁶⁸⁵Caldera Systems, Inc. Security Advisory, CSSA-2000-033.0, September 25, 2000.
- ⁶⁸⁶Red Hat, Inc. Security Advisory, RHSA-2000:065-04, October 4, 2000.
- ⁶⁸⁷Bugtraq, September 26, 2000.
- ⁶⁸⁸Conectiva Linux Security Announcement, 2000-07.27:gpm, July 27, 2000.
- ⁶⁸⁹Caldera Systems, Inc. Security Advisory, CSSA-2000-024.0, July 6, 2000.
- ⁶⁹⁰Red Hat, Inc. Security Advisory, RHSA-2000:045-01, July 26, 2000.
- ⁶⁹¹eSecurityOnline.com, October 4, 2000.
- ⁶⁹²Conectiva Linux Security Announcement, October 3, 2000.
- ⁶⁹³Red Hat, Inc. Security Advisory, RHSA-2000:072-07, November 2, 2000.
- ⁶⁹⁴Red Hat Inc. Security Advisory, RHSA-2000:110-06, November 20, 2000.
- ⁶⁹⁵Linux-Mandrake Security Update Advisory, MDKSA-2000:072, November 20, 2000.
- ⁶⁹⁶Debian Security Advisory, November 22, 2000.
- ⁶⁹⁷TurboLinux Security Announcement, TLSA2000018-1, August 9, 2000.
- ⁶⁹⁸SuSE Security Announcement, August 10, 2000.
- ⁶⁹⁹Red Hat, Inc. Security Advisory, RHSA-2000:048-02, August 8, 2000.
- ⁷⁰⁰Red Hat, Inc. Security Advisory, RHSA-2000:080-01, October 6, 2000.
- ⁷⁰¹Immunix OS Security Update, October 7, 2000.
- ⁷⁰²Linux-Mandrake Security Update Advisory, MDKSA-2000:056, October 7, 2000.
- ⁷⁰³Trustix Security Advisory, October 9, 2000.
- ⁷⁰⁴Conectiva Linux Security Announcement, October 9, 2000.
- ⁷⁰⁵Security Alert Consensus #054, July 20, 2000.
- ⁷⁰⁶Securiteam, August 8, 2000.
- ⁷⁰⁷ANSIR Advisory, May 19, 2000.
- ⁷⁰⁸Bugtraq, May 18, 2000.
- ⁷⁰⁹Securiteam, September 7, 2000.
- ⁷¹⁰Securiteam, September 10, 2000.
- ⁷¹¹Federico Schwindt, May 23, 2000.
- ⁷¹²Securiteam, June 8, 2000.
- ⁷¹³Securiteam, June 28, 2000.
- ⁷¹⁴NetBSD Security Advisory, 2000-008, July 10, 2000.
- ⁷¹⁵SuSE Security Announcement, July 11, 2000.

-
- ⁷¹⁶Linux-Mandrake Security Update, July 2, 2000.
⁷¹⁷Debian Security Advisory, Debian-00-026, September 11, 2000.
⁷¹⁸Conectiva Linux Security Announcement, September 11, 2000.
⁷¹⁹SuSE Security Announcement, September 13, 2000.
⁷²⁰Linux-Mandrake Security Update Advisory, MDKSA-2000:047, September 12, 2000.
⁷²¹Red Hat, Inc. Security Advisory, RHSA-2000:061-02, September 18, 2000.
⁷²²Linux-Mandrake Security Update Advisory, MDKSA-2000:050, September 18, 2000.
⁷²³Debian Security Advisory, 2000-9-19, September 19, 2000.
⁷²⁴Conectiva Linux Security Announcement, 2000-09-18, September 19, 2000.
⁷²⁵TurboLinux Security Announcement, TLSA2000022-2, September 19, 2000.
⁷²⁶Trustix Security Advisory, September 19, 2000.
⁷²⁷Caldera Systems, Inc. Security Advisory, CSSA-2000-032.0, September 19, 2000.
⁷²⁸SuSE Security Announcement, September 20, 2000.
⁷²⁹ISS E-Security Alert, February 1, 2000.
⁷³⁰Bugtraq, August 10, 2000.
⁷³¹Bugtraq, September 7, 2000.
⁷³²SilverBack Security Advisory, April 5, 2000.
⁷³³NetBSD Security Advisory, 2000-001, February 19, 2000.
⁷³⁴NetBSD Security Advisory, 2000-006, May 28, 2000.
⁷³⁵NetBSD Security Advisory, 1999-012, February 16, 2000.
⁷³⁶NetBSD Security Advisory, 2000-014, October 26, 2000.
⁷³⁷NHC 20000504a.0, May 4, 2000.
⁷³⁸Bugtraq, May 7, 2000.
⁷³⁹Delphis Consulting Plc Security Team Advisories, DST2K0031, September 21, 2000.
⁷⁴⁰Bugtraq, November 18, 2000.
⁷⁴¹eSecurityOnline.com Free Vulnerability Alert 3167, November 20, 2000.
⁷⁴²Securiteam, November 21, 2000.
⁷⁴³@stake Advisory, A091100-1, September 11, 2000.
⁷⁴⁴Bugtraq, June 21, 2000.
⁷⁴⁵Bugtraq, November 16, 2000.
⁷⁴⁶Security Advisory, Netopia R9100 DSL Router, May 8, 2000.
⁷⁴⁷SecurityFocus, January 16, 2000.
⁷⁴⁸Bugtraq, February 15, 2000.
⁷⁴⁹Securiteam, April 19, 2000.
⁷⁵⁰Securiteam, July 13, 2000.
⁷⁵¹S.A.F.E.R. Security Bulletin, 000317.EXP.1.5, March 17, 2000.
⁷⁵²Bugtraq, October 11, 2000.
⁷⁵³ACROS Security Problem Report, 2000-04-06-1-PUB, May 10, 2000.
⁷⁵⁴CERT, May 26, 2000.
⁷⁵⁵CORE SDI Security Advisory, CORE-2000103101, October 31, 2000.
⁷⁵⁶CORE SDI Security Advisory, CORE-2000103102, October 31, 2000.
⁷⁵⁷Securiteam, March 16, 2000.
⁷⁵⁸S.A.F.E.R. Security Bulletin, 000229.EXP.1.3, February 29, 2000.
⁷⁵⁹@stake, Inc. Security Advisory, A100900-1, October 9, 2000.
⁷⁶⁰Securiteam, March 16, 2000.
⁷⁶¹NTBugtraq, December 22, 1999.
⁷⁶²Securiteam, August 7, 2000.
⁷⁶³Securiteam, August 23, 2000.
⁷⁶⁴Bugtraq, July 24, 2000.
⁷⁶⁵Conectiva Linux Security Announcement, August 10, 2000.
⁷⁶⁶NetBSD Security Advisory 2000-011, August 10, 2000.
⁷⁶⁷SuSE Security Announcement, August 23, 2000.
⁷⁶⁸Bugtraq, November 24, 1999.
⁷⁶⁹Securiteam, January 3, 2000.
⁷⁷⁰Securiteam, June 24, 2000.

-
- ⁷⁷¹Bugtraq, June 29, 2000.
⁷⁷²Cerberus Information Security Advisory, CISADV000504, May 4, 2000.
⁷⁷³Bugtraq, June 21, 2000.
⁷⁷⁴Cerberus Information Security Advisory, CISADV000505, May 5, 2000.
⁷⁷⁵Bugtraq, June 2, 2000.
⁷⁷⁶Bugtraq, August 17, 2000.
⁷⁷⁷Bugtraq, June 23, 2000.
⁷⁷⁸Securiteam, May 27, 2000.
⁷⁷⁹ISN, May 23, 2000.
⁷⁸⁰SecurityFocus, May 22, 2000.
⁷⁸¹Bugtraq, June 18, 2000.
⁷⁸²CORE SDI Security Advisory, August 2, 2000.
⁷⁸³NTBugtraq, July 11, 2000.
⁷⁸⁴CERT Advisory CA-2000-18, August 24, 2000.
⁷⁸⁵SSR Labs Advisory, USSR-2000044, June 14, 2000.
⁷⁸⁶Securiteam, November 6, 2000.
⁷⁸⁷Bugtraq, November 22, 2000.
⁷⁸⁸Delphis Consulting Plc, May 5, 2000.
⁷⁸⁹Securiteam, June 21, 2000.
⁷⁹⁰RFP2K04, May 16, 2000.
⁷⁹¹L0pht Research Labs Security Advisory, L0pht-20000718, July 18, 2000.
⁷⁹²@stake Inc. Security Advisory, A101200-2, October 12, 2000.
⁷⁹³Bugtraq, November 27, 2000.
⁷⁹⁴Bugtraq, January 18, 2000.
⁷⁹⁵Bugtraq, February 25, 2000.
⁷⁹⁶USSR Labs, 2000031, January 13, 2000.
⁷⁹⁷Securiteam, July 7, 2000.
⁷⁹⁸Bugtraq, July 7, 2000.
⁷⁹⁹Bugtraq, December 19, 1999.
⁸⁰⁰SecurityFocus, February 7, 2000.
⁸⁰¹Bugtraq, June 26, 2000.
⁸⁰²Bugtraq, July 11, 2000.
⁸⁰³Bugtraq, April 18, 2000.
⁸⁰⁴Bugtraq, July 28, 2000.
⁸⁰⁵SecurityFocus, February 4, 2000.
⁸⁰⁶Network Computing Security Express #032, February 17, 2000.
⁸⁰⁷Securiteam, May 15, 2000.
⁸⁰⁸Bugtraq, January 9, 2000.
⁸⁰⁹Securiteam, July 25, 2000.
⁸¹⁰Bugtraq, October 11, 2000.
⁸¹¹FreeBSD Ports Security Advisory, FreeBSD-SA-00:65, November 6, 2000.
⁸¹²Securiteam, June 6, 2000.
⁸¹³SecurityFocus, April 24, 2000.
⁸¹⁴Bugtraq, October 4, 2000.
⁸¹⁵Bugtraq, October 5, 2000.
⁸¹⁶OpenBSD Security Advisory, October 4, 2000.
⁸¹⁷List Digest, October 10, 2000.
⁸¹⁸Linux-Mandrake Security Update Advisory, MDKSA-2000:068-1, November 15, 2000.
⁸¹⁹Trustix Security Advisory, November 15, 2000.
⁸²⁰Bugtraq, June 9, 2000.
⁸²¹Internet Security Systems Security Advisory, October 25, 2000.
⁸²²Securiteam, October 19, 2000.
⁸²³Cerberus Information Security Advisory, (CISADV000315), March 15, 2000.
⁸²⁴VIGILANTe Advisory, 2000002, July 4, 2000.
⁸²⁵Bugtraq, March 5, 2000.

⁸²⁶WWW.PLAZASITE.COM System & Security Division, 20001123, November 20, 2000.
⁸²⁷Securiteam, August 30, 2000.
⁸²⁸Cerberus Information Security Advisory , CISADV000717, July 17, 2000.
⁸²⁹Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2000-08, July 19, 2000.
⁸³⁰Red Hat, Inc. Security Advisory, RHSA-2000:024-02, October 27, 2000.
⁸³¹@stake, Inc Security Advisory, A092600- 1, September 27, 2000.
⁸³²Infosec Security Vulnerability Report, Infosec.20000617, June 17, 2000.
⁸³³DeepZone Security Advisory, April 17, 2000.
⁸³⁴Roe's Security Advisory, June 4, 2000.
⁸³⁵Bugtraq, July 9, 2000.
⁸³⁶Securiteam, August 10, 2000.
⁸³⁷Cerberus, May 25, 2000.
⁸³⁸Strumpf Noir Society Advisories, November 16, 2000.
⁸³⁹Securiteam, November 27, 2000.
⁸⁴⁰Bugtraq, November 23,2 000.
⁸⁴¹Secure Reality Pty Ltd. Security Advisory #, SRADV00001, September 4, 2000.
⁸⁴²Securiteam, June 16, 2000.
⁸⁴³SecurityFocus, January 5, 2000.
⁸⁴⁴Synnergy Laboratories Advisory SLA-2000-15, October 7, 2000.
⁸⁴⁵Bugtraq, June 2, 2000.
⁸⁴⁶Securiteam, March 24, 2000.
⁸⁴⁷Bugtraq, September 6, 2000.
⁸⁴⁸Securiteam, March 13, 2000.
⁸⁴⁹Securiteam, November 6, 2000.
⁸⁵⁰SecurityFocus, May 1, 2000.
⁸⁵¹Securiteam, January 18, 2000.
⁸⁵²USSR Labs Advisory Code, USSR-2000033, February 22, 2000.
⁸⁵³USSR Labs Advisory Code, USSR-2000034, February 24, 2000.
⁸⁵⁴USSR Labs Advisory Code, USSR-2000051, August 24, 2000.
⁸⁵⁵Bugtraq, February 3, 2000.
⁸⁵⁶Bugtraq, November 26, 2000.
⁸⁵⁷Securiteam, September 4, 2000.
⁸⁵⁸Bugtraq, April 14, 2000.
⁸⁵⁹Securiteam, December 24, 1999.
⁸⁶⁰SecurityFocus, April 28, 2000.
⁸⁶¹Bugtraq, May 15, 2000.
⁸⁶²buffer0verfl0w Security Advisory, b0f-SA2000-005, May 23, 2000.
⁸⁶³SecurityFocus, January 26, 2000.
⁸⁶⁴L0pht Research Labs Security Advisory, July 20, 2000.
⁸⁶⁵Securiteam, September 13, 2000.
⁸⁶⁶Bugtraq, September 11, 2000.
⁸⁶⁷Securiteam, August 19, 2000.
⁸⁶⁸SecuritySearch.net, June 5, 2000.
⁸⁶⁹USSR Advisory Code, USSR-2000038, April 20, 2000.
⁸⁷⁰Bugtraq, December 22, 1999.
⁸⁷¹Bugtraq, April 3, 2000.
⁸⁷²CORE SDI ADVISORY, CORE-20001116, November 17, 2000.
⁸⁷³Securiteam, March 11, 2000.
⁸⁷⁴Fate Research Labs Advisory, November 1, 2000.
⁸⁷⁵Red Hat, Inc. Security Advisory, RHSA-2000:062-03, September 19, 2000.
⁸⁷⁶Bugtraq, February 26, 2000.
⁸⁷⁷Red Hat, Inc. Security Advisory, RHSA-2000:059-02, September 11, 2000.
⁸⁷⁸Red Hat, Inc. Security Advisory, RHSA-2000:060-03, September 13, 2000.
⁸⁷⁹Red Hat Inc. Security Advisory, RHSA-2000:122-04, December 4, 2000.
⁸⁸⁰Bugtraq, September 9, 2000.

881 RedHat Inc. Security Advisory, RHSA-2000:014-10, April 24, 2000.
882 Red Hat, Inc. Security Advisory, RHSA-2000:087-02, October 18, 2000.
883 Bugtraq, May 1, 2000.
884 RedHat Security Advisory, RHSA-2000-001-03, January 7, 2000 update.
885 RedHat, Inc. Security Advisory, RHSA-2000:016-03, July 3, 2000.
886 Bugtraq, June 21, 2000.
887 Red Hat, Inc. Security Advisory, RHSA-2000:102-04, November 10, 2000.
888 Bugtraq, October 20, 2000.
889 Bugtraq, November 4, 2000.
890 Securiteam, June 16, 2000.
891 Red Hat, Inc. Security Advisory, RHSA-2000:047-03, August 7, 2000.
892 Securiteam, April 20, 2000.
893 RedHat Security Advisory, RHSA-2000:002-01, January 7, 2000.
894 Red Hat, Inc. Security Advisory, RHSA-2000:100-02, November 2, 2000.
895 Trustix Security Advisory, November 3, 2000.
896 Red Hat, Inc. Security Advisory, RHSA-2000:053-04, August 29, 2000.
897 Red Hat, Inc. Security Advisory, RHSA-2000:075-07, November 8, 2000.
898 Securiteam, March 7, 2000.
899 Securiteam, December 13, 2000.
900 Bugtraq, November 13, 2000.
901 Bugtraq, August 29, 2000.
902 Securiteam, September 14, 2000.
903 Cerberus Information Security Advisory, CISADV000524a, May 24, 2000.
904 Securiteam, July 25, 2000.
905 Bugtraq, October 30, 2000.
906 Bugtraq, November 10, 2000.
907 Delphis Internet Consulting Security Team, June 2, 2000.
908 Securiteam, September 14, 2000.
909 Bugtraq, February 25, 2000.
910 SecurityFocus, February 24, 2000.
911 SPS Advisory #37, June 27, 2000.
912 USSR Labs, USSR-99026, December 28, 1999.
913 MDMA Advisory, June 5, 2000.
914 Bugtraq, March 11, 2000.
915 Bugtraq, September 11, 2000.
916 SCO Security Bulletin, 2000.04, February 8, 2000.
917 Network Associates, Inc. Security Advisory, NAI-Feb152000-2: February 15, 2000.
918 CORE SDI Inc, CORE-092700, September 27, 2000.
919 Bugtraq, January 19, 2000.
920 Technotronic, December 21, 1999.
921 Bugtraq, December 27, 1999.
922 Bugtraq, December 30, 1999.
923 Bugtraq, December 21, 1999.
924 Network Associates Inc. Security Advisory, NAI-Feb152000, February 15, 2000.
925 Bugtraq, May 15, 2000.
926 Securiteam, September 17, 2000.
927 Sendmail Security, June 7 2000.
928 Bugtraq, April 21, 2000.
929 Bugtraq, December 21, 1999.
930 USSR Labs Advisory, USSR-20000046, June 16, 2000.
931 USSR Advisory Code, USSR-2000046, June 16, 2000.
932 SGI Security Advisory, 20000803-01-A, August 17, 2000.
933 SGI Security Advisory, 20000303-01-PX, March 28, 2000.
934 Network Associates, Inc. Advisory NAI-0016, March 7, 2000.
935 Securiteam, January 3, 2000.

-
- ⁹³⁶Bugtraq, April 12, 2000.
⁹³⁷SecurityFocus, March 3, 2000.
⁹³⁸SGI Security Advisory, May 22, 2000.
⁹³⁹Bugtraq, August 2, 2000.
⁹⁴⁰Bugtraq, August 2, 2000.
⁹⁴¹Bugtraq, August 2, 2000.
⁹⁴²Bugtraq, August 2, 2000.
⁹⁴³Bugtraq, August 3, 2000.
⁹⁴⁴Bugtraq, August 2, 2000.
⁹⁴⁵Silicon Graphics Inc. Security Advisory, June 20, 2000.
⁹⁴⁶SGI Security Advisory, 20000801-01-A, August 14, 2000.
⁹⁴⁷Bugtraq, August 15, 2000.
⁹⁴⁸Slashcode SA-00:00, September 29, 2000.
⁹⁴⁹Bugtraq, December 8, 2000.
⁹⁵⁰Delphis Consulting Plc Security Team Advisories, DST2K0035, September 22, 2000.
⁹⁵¹Delphis Consulting Plc Security Team Advisories, DST2K0036, September 22, 2000.
⁹⁵²Bugtraq, August 17, 2000.
⁹⁵³eSecurityOnline.com Free Vulnerability Alert 3178, November 27, 2000.
⁹⁵⁴Cerberus Information Security Advisory, (CISADV000313), March 13, 2000.
⁹⁵⁵SecurityFocus, January 4, 2000.
⁹⁵⁶Securiteam, November 30, 2000.
⁹⁵⁷Secure Reality Pty Ltd. Security Advisory #4, October 27, 2000.
⁹⁵⁸Bugtraq, April 23, 2000.
⁹⁵⁹Bugtraq, July 1, 2000.
⁹⁶⁰Bugtraq, October 11, 2000.
⁹⁶¹Securiteam, August 31, 2000.
⁹⁶²Bugtraq, March 24, 2000.
⁹⁶³SecurityFocus, February 21, 2000.
⁹⁶⁴Georgi Guninski Security Advisory #25, October 25, 2000.
⁹⁶⁵Sun Microsystems, Inc. Security Bulletin, #00198, October 24, 2000.
⁹⁶⁶Bugtraq, December 22, 1999.
⁹⁶⁷Securiteam, April 26, 2000.
⁹⁶⁸Securiteam, April 27, 2000.
⁹⁶⁹Securiteam, May 2, 2000.
⁹⁷⁰Bugtraq, June 14, 2000.
⁹⁷¹Sun Microsystems, Inc. Security Bulletin, #00199, November 29, 2000.
⁹⁷²Foundstone, Inc. Security Advisory, FS-082200-11-JWS, August 22, 2000.
⁹⁷³Sun Microsystems, Inc. Security Bulletin, #00196, August 7, 2000.
⁹⁷⁴Bugtraq, May 12, 2000.
⁹⁷⁵Sun Microsystems, Inc. Security Bulletin, #00194, March 29, 2000.
⁹⁷⁶Bugtraq, January 23, 2000.
⁹⁷⁷Securiteam, April 19, 2000.
⁹⁷⁸S.A.F.E.R. Security Bulletin, 000309.EXP.1.4, March 9, 2000.
⁹⁷⁹Foundstone, Inc. Security Advisory, FS-071000-5-JWS, July 10, 2000.
⁹⁸⁰CERT Advisory, CA-99-16, December 14, 1999.
⁹⁸¹Sun Microsystems, Inc. Security Bulletin, 00191, December 29, 1999.
⁹⁸²Securiteam, January 9, 2000.
⁹⁸³Securiteam, October 30, 2000.
⁹⁸⁴SuSE Security Announcement, May 2, 2000.
⁹⁸⁵Bugtraq, November 29, 2000.
⁹⁸⁶SuSE Security Announcement, uSE-SA :2000:042, October 18, 2000.
⁹⁸⁷SuSE Security Announcement, February 9, 2000.
⁹⁸⁸@stake Inc. Security Advisory, A090700-2, September 7, 2000.
⁹⁸⁹Bugtraq, September 21, 2000.
⁹⁹⁰SuSE Security Announcement, July 10, 2000.

-
- ⁹⁹¹@stake Inc. Security Advisory, A090700-3, September 7, 2000.
- ⁹⁹²Securiteam, May 4, 2000.
- ⁹⁹³SuSE Security, May 18, 2000.
- ⁹⁹⁴SuSE Security, May 29, 2000.
- ⁹⁹⁵SuSE Security Announcement, August 10, 2000.
- ⁹⁹⁶Infosec Security Vulnerability Report, Infosec.20000625, July 3, 2000.
- ⁹⁹⁷Securiteam, July 6, 2000.
- ⁹⁹⁸Bugtraq, January 28, 2000.
- ⁹⁹⁹Securiteam, November 3, 2000.
- ¹⁰⁰⁰Securiteam, December 21, 1999.
- ¹⁰⁰¹Securiteam, August 10, 2000.
- ¹⁰⁰²Bugtraq, March 17, 2000.
- ¹⁰⁰³Bugtraq, October 22, 2000.
- ¹⁰⁰⁴Bugtraq, June 14, 2000.
- ¹⁰⁰⁵SecurityFocus, April 5, 2000.
- ¹⁰⁰⁶Securiteam, May 19, 2000.
- ¹⁰⁰⁷Bugtraq, April 10, 2000.
- ¹⁰⁰⁸CORE SDI Security Advisory, CORE-20001023, October 23, 2000.
- ¹⁰⁰⁹SecurityFocus, February 9, 2000.
- ¹⁰¹⁰Securiteam, February 18, 2000.
- ¹⁰¹¹Sword & Shield Enterprise Security, Inc. Security Advisory, April 12, 2000.
- ¹⁰¹²Delphis Consulting Plc Security Team Advisories, DST2K0042, September 26, 2000.
- ¹⁰¹³Delphis Consulting Plc Security Team Advisories, DST2K0032, September 19, 2000.
- ¹⁰¹⁴Bugtraq, August 2, 2000.
- ¹⁰¹⁵BluePanda Vulnerability Announcement, July 21, 2000.
- ¹⁰¹⁶Bugtraq, November 27, 2000.
- ¹⁰¹⁷BluePanda Vulnerability Announcement, July 7, 2000.
- ¹⁰¹⁸Blue Panda Vulnerability Announcement, September 5, 2000.
- ¹⁰¹⁹FreeBSD Security Advisory: FreeBSD-SA-00:06.htdig, March 1, 2000.
- ¹⁰²⁰Geekgang Security Advisory, gsa2000-01, October 26, 2000.
- ¹⁰²¹Securiteam, December 29, 1999.
- ¹⁰²²403-SECURITY advisory, November 21, 2000.
- ¹⁰²³Alcatel Security Advisory, December 27, 1999.
- ¹⁰²⁴Network Associates, Inc. COVERT Labs Security Advisory, May 4, 2000.
- ¹⁰²⁵Bugtraq, November 28, 2000.
- ¹⁰²⁶Bugtraq, December 30, 1999.
- ¹⁰²⁷Bugtraq, February 25, 2000.
- ¹⁰²⁸Bugtraq, March 22, 2000.
- ¹⁰²⁹Bugtraq, April 17, 2000.
- ¹⁰³⁰Bugtraq, November 30, 2000.
- ¹⁰³¹SecurityFocus, February 10, 2000.
- ¹⁰³²SecurityFocus, February 10, 2000.
- ¹⁰³³Bugtraq, December 27, 1999.
- ¹⁰³⁴Securiteam, August 16, 2000.
- ¹⁰³⁵eSecurityOnline.com Free Vulnerability Alert 3149, November 15, 2000.
- ¹⁰³⁶Bugtraq, August 10, 2000.
- ¹⁰³⁷TurboLinux Advisory ID#: TLSA200007-1, March 15, 2000.
- ¹⁰³⁸Turbo Linux Security Announcement, TLSA2000009-1, April 14, 2000.
- ¹⁰³⁹Bugtraq, May 3, 2000.
- ¹⁰⁴⁰Bugtraq, June 8, 2000.
- ¹⁰⁴¹Bugtraq, November 21, 2000.
- ¹⁰⁴²Foundstone, Inc. Security Advisory, FS-103000-15-SRVX, October 30, 2000.
- ¹⁰⁴³Foundstone, Inc. Security Advisory, FS-103100-16-SRVX, October 31, 2000.
- ¹⁰⁴⁴Bugtraq, February 27, 2000.
- ¹⁰⁴⁵Securiteam, August 25, 2000.

-
- ¹⁰⁴⁶Guardent Security Advisory, A0208102000, August 10, 2000.
¹⁰⁴⁷SecurityFocus, April 20, 2000.
¹⁰⁴⁸Securiteam, December 14, 2000.
¹⁰⁴⁹eSecurityOnline.com, September 26, 2000.
¹⁰⁵⁰SecurityPortal, 2000-07-14, July 24, 2000.
¹⁰⁵¹Bugtraq, January 21, 2000.
¹⁰⁵²Securiteam, March 24, 2000.
¹⁰⁵³Bugtraq, March 15, 2000.
¹⁰⁵⁴Tamandua Sekure Labs, Sekure-2000-01, October 25, 2000.
¹⁰⁵⁵Bugtraq, October 16, 2000.
¹⁰⁵⁶Bugtraq, October 25, 2000.
¹⁰⁵⁷Securiteam, June 18, 2000.
¹⁰⁵⁸Bugtraq, July 14, 2000.
¹⁰⁵⁹Bugtraq, July 5, 2000.
¹⁰⁶⁰Bugtraq, January 24, 2000.
¹⁰⁶¹eSecurityOnline.com Free Vulnerability Alert 3124, November 8, 2000.
¹⁰⁶²Vapid Labs Advisory, 10132000-01, November 7, 2000.
¹⁰⁶³F8 labs Advisory, 20001205, December 6, 2000.
¹⁰⁶⁴Fate Research Labs, December 5, 2000.
¹⁰⁶⁵Securiteam, August 27, 2000.
¹⁰⁶⁶Securiteam, March 27, 2000.
¹⁰⁶⁷Bugtraq, January 19, 2000.
¹⁰⁶⁸Vigilante Advisory, VIGILANTE-2000005, August 15, 2000.
¹⁰⁶⁹Securiteam, November 19, 2000.
¹⁰⁷⁰Securiteam, December 15, 2000.
¹⁰⁷¹USSR Labs Advisory, USSR-2000047, June 16, 2000.
¹⁰⁷²Delphis Consulting Plc Security Team Advisories, DST2K0039, September 26, 2000.
¹⁰⁷³Securiteam, January 6, 2000.
¹⁰⁷⁴USSR Advisory Code, USSR-2000048, July 4, 2000.
¹⁰⁷⁵Blue Panda Vulnerability Announcement, October 2, 2000.
¹⁰⁷⁶USSR Advisory Code, USSR-2000049, July 10, 2000.
¹⁰⁷⁷Bugtraq, July 13, 2000.
¹⁰⁷⁸SecurityFocus, February 3, 2000.
¹⁰⁷⁹Securiteam, December 29, 1999.
¹⁰⁸⁰Bugtraq, January 20, 2000.
¹⁰⁸¹Delphis Consulting Plc Security Advisory, DST2K0023, August 25, 2000.
¹⁰⁸²Delphis Consulting Plc Security Team Advisories, DST2K0037, September 28, 2000.
¹⁰⁸³Delphis Consulting Plc Security Team Advisories, DST2K0040, October 6, 2000.
¹⁰⁸⁴Caldera Systems, Inc. Security Advisory, CSSA-2000-012.0, May 18, 2000.
¹⁰⁸⁵eSecurityOnline.com, October 4, 2000.
¹⁰⁸⁶Securiteam, October 17, 2000.
¹⁰⁸⁷Rootshell, June 2, 2000.
¹⁰⁸⁸Linux-Mandrake Security Update Advisory, MDKSA-2000:041, August 29, 2000.
¹⁰⁸⁹Securiteam, September 1, 2000.
¹⁰⁹⁰Bugtraq, September 10, 2000.
¹⁰⁹¹Securiteam, November 8, 2000.
¹⁰⁹²USSR Labs, USSR-99024, December 23, 1999.
¹⁰⁹³Sword & Shield Enterprise Security, Inc. Security Advisory, May 10, 2000.
¹⁰⁹⁴S.A.F.E.R. Security Bulletin 000209.EXP.1.2, February 9, 2000.
¹⁰⁹⁵Ernst & Young eSecurity, June 15, 2000.
¹⁰⁹⁶SecurityFocus, April 24, 2000.
¹⁰⁹⁷SecurityFocus, January 7, 2000.
¹⁰⁹⁸Zope Security Alert, June 15, 2000.
¹⁰⁹⁹Bugtraq, June 16, 2000.
¹¹⁰⁰RedHat, Inc. Security Advisory, RHSA-2000:038-01, June 22, 2000.