



Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-10

May 19, 2003

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

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

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

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 30 and May 16, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com ¹	Multiple	Office Connect DSL Router 812 1.1.7, 1.1.9	A vulnerability exists due to a flaw in the way DHCP traffic is handled, which could let a malicious user obtain sensitive information.	Upgrade available at: ftp://ftp.3com.com/pub/officeconnect/ocradsl/bld_1_1_9_4.zip	OfficeConnect ADSL Router DHCP Traffic	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Adobe Systems, Inc. ²	Windows	Acrobat 5.0, 5.0.5	An input validation vulnerability exists in the JavaScript parsing engine, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www.adobe.com/support/downloads/thankyou.jsp?ftpID=2121&fileID=2065	Acrobat JavaScript Parsing Engine	High	Bug discussed in newsgroups and websites.

¹ Bugtraq, May 14, 2003.

² Adobe Security Advisory, May 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple ³	MacOS X	Safari Beta2	A vulnerability exists because the Common Name (CN) field on X.509 certificates is not properly validated when a SSL/TLS session is negotiated, which could let a malicious server masquerade as a trusted server.	No workaround or patch available at time of publishing.	Safari Common Name Certificate Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple ⁴	Multiple	AirPort Base Station	A vulnerability exists due to a weak XOR algorithm used to encrypt authentication credentials, which could let a malicious user obtain sensitive information	Workaround: Apple has recommended that users administrate the AirPort device through wired media where possible.	AirPort Administrative Password Encryption Weakness CVE Name: CAN-2003-0270	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
BEA Systems Inc. ⁵	Windows NT 4.0/2000, Unix	WebLogic Express 7.0.0.1, 7.0.0.1 SP1&SP2, 7.0, 7.0 SP1&SP2, WebLogic Express for Win32 7.0.0.1, 7.0.0.1 SP1&SP2, Win32 7.0, 7.0 SP1&SP2, Weblogic Server 7.0.0.1, 7.0.0.1 SP1&SP2, 7.0, 7.0 SP1&SP2, WebLogic Server for Win32 7.0.0.1, 7.0.0.1 SP1&SP2, 7.0, 7.0 SP1&SP2,	Multiple vulnerabilities exist: a vulnerability exists due to the way some passwords are stored in the 'CredentialMapper,' which could let a malicious user obtain sensitive information and unauthorized access; a vulnerability exists in the 'config.xml,' 'firerealm.properties,' and 'weblogic-rar.xml' files because details about the encryption of passwords is available, which could let a malicious user obtain sensitive information; and a vulnerability exists in 'JDBCConnectionPool RuntimeMBean' because the password of privileged users may be displayed in plain text on the screen of a user logged in to the administrative interface, which could let a malicious user obtain sensitive information.	Patches available at: ftp://ftpna.beasys.com/pub/releases/security/CR104520_700sp2.zip	WebLogic Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

³ Bugtraq, May 7, 2003.

⁴ @stake, Inc. Security Advisory, a051203-1), May 12, 2003.

⁵ BEA Security Advisory, BEA03-30.00, May 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Best Practical Solutions ⁶	Unix	RT 1.0.0-1.0.7	A vulnerability exists due to insufficient sanitization of user-supplied values in message bodies, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: http://www.fस्क.com/pub/rt/release/rt-3-0-1.tar.gz	RT Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.
BitchX ⁷	Multiple	IRC Client 1.0 c20cvs	A Denial of Service vulnerability exists when certain mode changes are made.	Upgrade available at: ftp://ftp.bitchx.org/pub/BitchX/cvs-snapshot/bx1.0c20-cvs-05092003.tar.gz	BitchX Mode Change Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Boa ⁸	Unix	Boa Webserver 0.92 r	A file disclosure vulnerability exists due to insufficient sanitization of user-supplied HTTP requests, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.boa.org/boa-0.94.13.tar.gz	Boa Webserver File Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
BVRP Software ⁹	Windows NT 4.0/2000	SLWeb Mail 5.1.0.4420	Several vulnerabilities exist: a Directory Traversal vulnerability exists in the administrative web interface, which could let a remote malicious user obtain sensitive information or execute arbitrary commands; and an information disclosure vulnerability exists in the administrative interface, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.slmail.com	SLMail Administrative Interface Directory Traversal & Information Disclosure	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

⁶ SecurityTracker Alert ID, 1006750, May 14, 2003.

⁷ Bugtraq, May 10, 2003.

⁸ Securiteam, May 12, 2003.

⁹ NGSSoftware Insight Security Research Advisory, May 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BVRP Software ¹⁰	Windows NT 4.0/2000	SLWeb Mail 3	Multiple vulnerabilities exist: buffer overflow vulnerabilities exist in 'showlogin.dll,' 'admin.dll,' 'recman.dll,' and 'globallogin.dll' when certain malformed URL requests are sent, which could let a malicious user cause a Denial of Service or execute arbitrary code; a vulnerability exists when invalid request are submitted to certain DLLs, which could let a malicious user obtain sensitive information; a buffer overflow vulnerability exists when a string of excessive length is submitted to the 'POPPasswd' service, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in multiple libraries due to insufficient bounds checking when processing the 'LANGUAGE' variable, which could let a malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'ETRN' command due to insufficient bounds checking, which could let a malicious user execute arbitrary code; a remote Denial of Service vulnerability exists in several of the GUI applications; and several path disclosure vulnerabilities exist when the 'LANGUAGE' variable is set to something invalid, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.smail.com	SLWebmail Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required for the ISAPI DLL buffer overflows.
Caldera ¹¹	Unix	OpenLinux Server 3.1, 3.1.1, Workstation 3.1, 3.1.1	A vulnerability exists in tcp_sec implementations due to the way TCP packets are filtered, which could let a malicious user bypass network firewall policies.	Upgrade available at: ftp://ftp.sco.com/pub/updates/OpenLinux/	OpenLinux TCP_Sec TCP Packet Filtering	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁰ NGSSoftware Insight Security Research Advisory, May 7, 2003.

¹¹ SCO Security Advisory, CSSA-2003-019.0, May 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Carl-Fredrik Neikter ¹²	Windows	Netbus 1.5-1.7	A vulnerability exists when a connection is made from a host further connections from that IP address may not need to authentic, which could let a remote malicious user bypass authentication mechanism.	No workaround or patch available at time of publishing.	Netbus Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a Netbus client.
CDR Tools ¹³	Unix	CDRecord 1.11, 2.0	A format string vulnerability exists due to a programming error when the 'printf-like' function is called, which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: ftp://ftp.berlios.de/pub/cdrecord/alpha/cdrttools-2.01a14.tar.gz Mandrake: http://www.mandrakesecure.net/en/ftp.php	CDRecord 'printf-like' Format String	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Cerberus ¹⁴	Windows NT	FTP Server 2.1	A vulnerability exists because authentication credentials are stored in plaintext, which could let a malicious user obtain sensitive information and unauthorized access.	No workaround or patch available at time of publishing.	FTP Server Plaintext Password Weakness	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Charles DeWeese ¹⁵	Windows	FlashFXP 1.4	A vulnerability exists due to a weak password encryption algorithm, which could let a malicious user obtain sensitive information.	This issue has been addressed through the Application Password Protection feature in FlashFXP version 2.0. Users should contact the vendor for details on obtaining this version.	FlashFXP User Password Encryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco Systems ¹⁶	Multiple	ONS 15327 3.0-3.4, ONS 15454 Optical Transport Platform, 3.0-3.4, 15454SDH 3.1-3.4, ONS 15600 1.0	Denials of Service vulnerabilities exist when a malicious user submits invalid requests to the FTP and Telnet services.	Upgrade available at: http://www.cisco.com/tac	Optical Transport Platform Invalid FTP & Telnet Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited with the Nessus VxWorks FTP DoS script and the VxWorks binlogin overflow script.

¹² SecurityTracker Alert ID, 1006736, May 10, 2003.

¹³ Mandrake Linux Security Update Advisory, MDKSA-2003:058, May 15, 2003.

¹⁴ SecurityFocus, May 12, 2003.

¹⁵ SecurityTracker Alert ID, 1006730, May 8, 2003.

¹⁶ Cisco Security Advisory, May 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ¹⁷	Windows	VPN Client 3.0 for Windows, 3.0.5 for Windows, 3.1 for Windows, 3.5.1 C for Windows, 3.5.1 for Windows, 3.5.2 B for Windows, 3.5.2 for Windows, 3.5.4 for Windows, 3.6 (Rel) for Windows, 3.6 for Windows, 3.6.1 for Windows	A vulnerability exists when the VPN client is set to start prior to logon, which could let a malicious user obtain elevated privileges.	Workaround available at: http://www.cisco.com/warp/public/707/vpnclient-multiple2-vuln-pub.shtml	Cisco VPN Client Elevated Privileges	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems ¹⁸	Multiple	VPN 3000 Concentrat or 3.5 (Rel), 3.5.1-3.5.5, 3.6, 3.6.1, 3.6.7 D, 4.0, 3002 Hardware Client, 3005 Concentra- tor 3.6.3, 3.6.5, 3.6.7- 3.6.7D, 4.0, 4.0.1, 3015 Concentra- tor, 3030 Concentrat or, 3060 Concentra- tor, 3080 Concentra- tor	Multiple vulnerabilities exist: a vulnerability exists because incoming traffic that is on a port designed to send IPSec over TCP is not properly handled, which could let a malicious user obtain unauthorized access; a Denial of Service vulnerability exists in the SSH server when a malicious user submits certain malformed SSH session initialization packets; and a Denial of Service vulnerability exists when a malicious user floods the server with certain types of ICMP traffic.	Upgrades available at: http://www.cisco.com	VPN Concentrator Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.

¹⁷ NTBugtraq, May 14, 2003.

¹⁸ Cisco Security Advisory, May 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ¹⁹ <i>Cisco releases patch²⁰</i>	Multiple	Catalyst 4000 7.5 (1), 6000 7.5 (1), 6500 7.5 (1)	A vulnerability exists due to the way the 'enable' mode is accessed, which could let a remote malicious user obtain elevated privileges.	<i>Upgrade available at: http://www.cisco.com/warp/public/707/cisco-sa-20030424-catos.shtml</i>	CatOS Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Clearswift Limited ²¹	Windows 2000	Mail Sweeper 4.0-4.3.7	A vulnerability exists due to the way attachment filenames are handled, which could let a malicious user bypass filtering mechanisms.	Upgrade available at: http://www.clearswift.com	MailSweeper Attachment Filename Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Clearswift Limited ²²	Windows 2000	Mail Sweeper 4.3.6, 4.3.7	Two vulnerabilities exist: a remote Denial of Service vulnerability exists when PowerPoint files that contain malformed attributes are handled; and a vulnerability exists in the File Blocker because some attachments are not blocked if the attachment file name consists of multiple extensions combined with large blocks of white spaces, which could let a remote malicious user bypass File Blocking filters.	Patch available at: http://www.clearswift.com/download/bin/Patches/ReadMe_SMTTP_438.htm	MailSweeper PowerPoint File Denial of Service & Filter Bypass	Low/ Medium (Medium if file blocking filters can be bypassed)	Bug discussed in newsgroups and websites. There is no exploit code required.
CREN ²³	Unix	ListProc 8.2.9	A buffer overflow vulnerability exists in the 'ULISTPROC_UMASK' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ListProc ULISTPROC_UMASK Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Darkwet Network ²⁴	Windows	WebCam XP 1.2.432, XP 1.2.535	Input validation vulnerabilities exist in the web-based chat feature due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	WebcamXP Message Field HTML Code Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Dr. Jay Stockman ²⁵	Multiple	Stockman Shopping Cart 7.8	A vulnerability exists in the 'shop/plx' script due to insufficient sanitization of user-supplied URI parameters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Stockman Shopping Cart Arbitrary Command Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁹ Cisco Security Advisory, Revision 1, April 25, 2003.

²⁰ Cisco Security Advisory, Revision 1.3, May 7, 2003.

²¹ SecurityFocus, May 13, 2003.

²² SecurityFocus, May 12, 2003.

²³ Secure Network Operations, Inc. Advisory, SRT2003-05-08-1137, May 8, 2003.

²⁴ Frame4 Security Advisory, FSA-2003:002, May 2, 2003.

²⁵ SecurityFocus, May 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ethereal Group ²⁶	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Ethereal 0.8, 0.8.18, 0.9.0-0.9.11	Buffer overflow vulnerabilities exist in several dissectors that are included with Ethereal due to integer overflows and off-by-one errors, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.ethereal.com/distribution/ethereal-0.9.12.tar.gz	Ethereal Multiple Dissector Buffer Overflows	High	Bug discussed in newsgroups and websites.
Etype ²⁷	Windows 95/98/NT 4.0/2000, XP	Eserv 2.92-2.99	A remote Denial of Service vulnerability exists due to a memory leak in the connection routine.	Contact the vendor for upgrade information.	EServ Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Floosietek ²⁸	Windows	FTGatePro 1.22 (1328)	Several vulnerabilities exists: a buffer overflow vulnerability exists when the mail server attempts to process overly long SMTP 'Mail From' arguments, which could let a remote malicious user cause a Denial of Service and execute arbitrary code; and a buffer overflow vulnerability exists when the mail server attempts to process overly long SMTP 'Rcpt To' arguments, which could let a malicious user execute arbitrary code.	Hotfix available at: http://www.ftgate.com/content/44.htm	FTGate PRO Multiple Buffer Overflows	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi ²⁹	Windows, Unix	PHP-Nuke 5.0-5.6, 6.0, 6.5 RC1-RC3, 6.5 Final, 6.5 Beta 1, 6.5	Multiple input validation vulnerabilities exist in the 'Web_Links' module, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPNuke Web_Links Module Remote SQL Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi ³⁰	Windows, Unix	PHP-Nuke 6.5, 6.5 RC1-RC3, 6.5 Final	A Cross-Site Scripting vulnerability exist in the 'modules.php' script due to insufficient sanitization of the 'username' URI parameter, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHP-Nuke 'Modules.PHP' Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

²⁶ Ethereal Security Advisory, enpa-sa-00009, May 3, 2003.

²⁷ Securiteam, May 12, 2003.

²⁸ Bugtraq, May 6, 2003.

²⁹ 7 A 6 9 - Adv, May 11, 2003.

³⁰ Bugtraq, May 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi ³¹	Windows, Unix	PHP-Nuke 6.0, 6.5, 6.5 RC1-RC3, 6.5 Final, 6.5 Beta 1	A path disclosure vulnerability exists in the 'Web_Links' module, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP-Nuke Web_Links Module Path Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi ³²	Windows, Unix	PHP-Nuke 6.5, 6.5 RC1-RC3, 6.5 Final, 6.5 Beta 1	Multiple SQL injection vulnerabilities exist in the 'Downloads' module, which could let a remote malicious user execute arbitrary SQL code.	No workaround or patch available at time of publishing.	PHP-Nuke Multiple Downloads Module SQL Injection Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit has been published.
Fuzz ³³	Unix	Fuzz 0.6	A vulnerability exists due to the creation of insecure temporary files, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://security.debian.org/pool/updates/main/f/fuzz/	Fuzz Privilege Escalation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
GNU ³⁴	Unix	GNU Privacy Guard 1.0-1.2.1	A vulnerability exists in the key validation code due to insufficient differentiation between the validity given to individual IDs on a public key that has multiple user IDs linked to it, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.gnupg.org/(en)/download/index.html#auto-ref-0	GNU Privacy Guard Insecure Trust Path To User ID	Medium	Bug discussed in newsgroups and websites.
Happycgi.com ³⁵	Unix	HappyMall 4.3, 4.4	A vulnerability exists in the 'normal_html.cgi' and 'member_html.cgi' scripts due to insufficient filtering of user-supplied input, which could let a remote malicious user execute arbitrary commands.	Patch available at: http://happymall.happycgi.com/forum/forum_detail.cgi?thread=353	HappyMall E-Commerce Software Remote Arbitrary Command Execution CVE Name: CAN-2003-0243	High	Bug discussed in newsgroups and websites. Exploits have been published.
Hewlett Packard Company ³⁶	Unix	HP-UX 10.x, 11.x	A buffer overflow vulnerability exists in the 'rwrite' utility due to insufficient bounds checking, which could let a malicious user obtain elevated privileges and possibly execute arbitrary code.	Patch available at: http://itrc.hp.com	HP-UX RWrite Buffer Overflow	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

³¹ Bugtraq, May 12, 2003.

³² 7 A 6 9 – Adv, May 13, 2003.

³³ Debian Security Advisory, DSA 302-1, May 7, 2003.

³⁴ Bugtraq, May 4, 2003.

³⁵ Korean CERT Advisory, KA-2003-33, May 3, 2003.

³⁶ Bugtraq, May 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company ³⁷ <i>Upgrade now available</i> ³⁸	Unix	HP-UX 11.0 4, 11.0, 11.11, 11.20	A buffer overflow vulnerability exists when an excessive amount of data is redirected into wall as a message intended to be broadcast, which could let a remote malicious user execute arbitrary code.	<i>Upgrade available at:</i> ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/	HPUX Wall Message Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
IBM ³⁹	Unix	AIX 4.3-4.3.3, 5.1 L, 5.1, 5.2	A vulnerability exists in the default Sendmail configuration, which could let a remote malicious user obscure the origins of e-mail.	No workaround or patch available at time of publishing.	AIX Sendmail Default Configuration Weakness	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Info-ZIP ⁴⁰	Unix	UnZip 5.5	A Directory Traversal vulnerability exists during the handling of pathnames for archived files, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	UnZip Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Inktomi ⁴¹	Unix	Traffic Server 4.0.18, 4.0.20, 5.1.3, 5.2.0-R, 5.2.1, 5.2.2	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of proxy input, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Inktomi Traffic Server Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
IP Messenger ⁴²	Windows	IP Messenger For Win 2.0-2.0.2	A buffer overflow vulnerability exists due to insufficient bounds checking of the filename, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.asahi-net.or.jp/~VZ4H-SRUZ/ipmsg203.zip	IP Messenger Filename Buffer Overflow	High	Bug discussed in newsgroups and websites.
IU Blog ⁴³	Multiple	IU Blog	A vulnerability exists in the 'Comment Form' due to insufficient sanitization of encoded character HTML tags, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	IU BLog Comment Form Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.

³⁷ Bugtraq, February 7, 2003.

³⁸ Hewlett-Packard Company Security Bulletin, HPSBUX0305-258, May 7, 2003.

³⁹ SDSC Security Note, May 13, 2003.

⁴⁰ Bugtraq, May 10, 2003.

⁴¹ Bugtraq, May 14, 2003.

⁴² SNS Advisory No.64, May 13, 2003.

⁴³ SecurityFocus, May 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jelsoft Enterprises ⁴⁴	Windows, Unix	VBulletin 3.0 beta 2	A vulnerability exists due to insufficient sanitization of private messages, which could let a malicious user execute arbitrary HTML or script code.	Users are advised to upgrade to the latest 3.0 beta version. Further information regarding how to obtain the latest version can be obtained by contacting the vendor.	VBulletin Private Message	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Joel Palmius ⁴⁵	Windows, Unix	mod_survey 3.0-3.0.15-pre6	A remote Denial of Service vulnerability exists due to a design error when handling nonexistent survey names.	Upgrade to 3.0.15 available at; http://gathering.itm.mh.se/modsurvey/download.php	Mod_Survey SYSBASE Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
K. Agusa & S. Yamamoto ⁴⁶	Unix	youbin 2.5, 3.0, 3.4	A buffer overflow vulnerability exists in the 'HOME' environment variable due to insufficient bound checking, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	Youbin HOME Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
KDE ⁴⁷	Unix	kopete 0.6.1	A vulnerability exists in the GnuPG plugin due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary commands.	Mandrake: http://www.mandrakesecure.net/en/ftp.php	Kopete GnuPG Plugin Remote Command Execution CVE Name: CAN-2003-0256	High	Bug discussed in newsgroups and websites.
KDE ⁴⁸	Unix	Konqueror Embedded 0.1	A vulnerability exists because the Common Name (CN) field on X.509 certificates is not properly validated when a SSL/TLS session is negotiated, which could let a malicious server masquerade as a trusted server.	No workaround or patch available at time of publishing.	Konqueror Embedded Common Name Certificate Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
KDE ⁴⁹	Unix	Konqueror 3.0.3	A Denial of Service vulnerability exists when rendering a HTML page that contains malformed data. The execution of arbitrary code may also be possible.	No workaround or patch available at time of publishing.	KDE Konqueror Malformed HTML Page Denial of Service	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁴⁴ Bugtraq, May 14, 2003.

⁴⁵ Securiteam, May 5, 2003.

⁴⁶ Secunia Security Advisory, May 7, 2003.

⁴⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:055, May 8, 2003.

⁴⁸ Bugtraq, May 7, 2003.

⁴⁹ Bugtraq, May 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KDE ^{50, 51} <i>More patches released^{52, 53}</i> <i>Conectiva releases patches⁵⁴</i> <i>RedHat releases patches⁵⁵</i>	Unix	KDE 2.0, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5	Multiple vulnerabilities exist due to a failure to properly quote parameters of instructions passed to a command shell for execution, which could let a local/remote malicious user execute arbitrary commands.	Upgrade available at: http://download.kde.org/stable/3.0.5a/ <i>Debian:</i> http://security.debian.org/pool/updates/main/k/kdeadmin/ <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br/ <i>RedHat:</i> ftp://updates.redhat.com/	KDE Parameter Quoting Shell Command Execution CVE Name: CAN-2002-1393	High	Bug discussed in newsgroups and websites.
KDE ^{56, 57, 58} <i>More updates issued^{59, 60, 61, 62}</i> <i>RedHat releases update⁶³</i>	Unix	KDE 2.0-3.1.1	A vulnerability exists when specially formatted PDF and PS files are processed due to the way the Ghostscript software is used, which could let a malicious user execute arbitrary commands.	<i>KDE:</i> http://download.kde.org/stable/3.0.5b/ <i>Debian:</i> http://security.debian.org/pool/updates/main/k/kdegraphics/ <i>Mandrake:</i> http://www.mandrakesecurity.net/en/ftp.php <i>SuSE:</i> ftp://ftp.suse.com/pub/suse <i>Debian:</i> http://security.debian.org/pool/updates/main/k/kdelibs/ http://security.debian.org/pool/updates/main/k/kdebase/kde <i>RedHat:</i> ftp://updates.redhat.com/	KDE Postscript/PDF File Processing CVE Name: CAN-2003-0204	High	Bug discussed in newsgroups and websites.
Kerio Technologies ⁶⁴ <i>More exploit scripts published⁶⁵</i>	Windows	Personal Firewall 2 2.1-2.1.4	A buffer overflow vulnerability exists during the administration authentication process, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Personal Firewall Remote Authentication Buffer Overflow	High	Bug discussed in newsgroups and websites. <i>Proofs of Concept exploit scripts have been published.</i>

⁵⁰ KDE Security Advisory, December 21, 2002.

⁵¹ Gentoo Linux Security Announcement, 200212-9, December 22, 2002.

⁵² Gentoo Linux Security Announcement, 200301-11, January 18, 2003.

⁵³ Debian Security Advisories, DSA 234-1- 238-1, January 22 & 23, 2003.

⁵⁴ Conectiva Linux Security Announcement, CLA-2003:569, February 20, 2003.

⁵⁵ Red Hat Security Advisory, RHSA-2003:002-01, May 12, 2003.

⁵⁶ KDE Security Advisory, April 9, 2003.

⁵⁷ Debian Security Advisory, DSA 284-1, April 12, 2003.

⁵⁸ Sorcerer Update Advisory SORCERER2003-04-12, April 12, 2003.

⁵⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:049, April 17, 2003.

⁶⁰ SuSE Security Announcement, SuSE-SA:2003:0026, April 24, 2003.

⁶¹ Debian Security Advisory, DSA 293-1, April 23, 2003.

⁶² Debian Security Advisory, DSA 296-1, April 30, 2003.

⁶³ Red Hat Security Advisory, RHSA-2003:002-01, May 12, 2003.

⁶⁴ Core Security Technologies Advisory, CORE-2003-0305-02, April 28, 2003.

⁶⁵ SecurityFocus, May 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Kerio Technologies ⁶⁶	Windows	Personal Firewall 2.1-2.1.4	A vulnerability exists because fragmented packets are not properly handled, which could let a malicious user bypass existing firewall filters.	No workaround or patch available at time of publishing.	Kerio Personal Firewall Fragmented Packet Filter Bypass	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Laurent Duveau ⁶⁷	Windows, Unix	MiniPortail 1.9, 2.0-2.2	A vulnerability exists in the 'admin/admin.php' script due to the authentication procedure used, which could let a remote malicious user bypass authentication to obtain administrative access.	No workaround or patch available at time of publishing.	MiniPortail admin.PHP Authentication Bypass	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Leksbot ⁶⁸	Unix	Leksbot 1.2	Multiple vulnerabilities exist because the /usr/bin/KATAXWR program was inadvertently installed setuid root, which could let a malicious user obtain root privileges.	Upgrades available at: http://security.debian.org/pool/updates/main/l/leksbot/	Leksbot Multiple Unspecified Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Lgames ⁶⁹	Unix	LTris 1.0.1	A buffer overflow vulnerability exists in the 'HOME' environment variable, which could let a malicious user execute arbitrary code with privileges of the "games" group.	No workaround or patch available at time of publishing.	LTris Local Memory Corruption	High	Bug discussed in newsgroups and websites. Exploit script has been published.
MDG Computer Services ⁷⁰	Windows NT 4.0/2000, XP, MacOS	Web Server 4D 3.6	A buffer overflow vulnerability exists when an overly long HTTP GET request is submitted, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Web Server 4D HTTP Command Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft ⁷¹	Multiple	MN-500	A vulnerability exists in the configuration backup file because administrative passwords are stored in plaintext, which could let a remote malicious user obtain administrative credentials.	No workaround or patch available at time of publishing.	Microsoft MN-500 Plaintext Password Disclosure	High	Bug discussed in newsgroups and websites. There is no exploit code required.

⁶⁶ Bugtraq, May 8, 2003.

⁶⁷ Secunia Security Advisory, May 9, 2003.

⁶⁸ Debian Security Advisory, DSA 299-1, May 6, 2003.

⁶⁹ Bugtraq, May 8, 2003.

⁷⁰ SP Research Labs Advisory x05, April 30, 2003.

⁷¹ SecurityTracker Alert ID, 1006691, May 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷² <i>Proof of Concept exploits published</i> ⁷³	Windows 2000, XP	BizTalk Server 2000 Developer Edition, SP1a, SP2, 2000 Enterprise Edition, SP1a, SP2, 2000 Standard Edition, SP1a, SP2, 2002 Developer Edition, 2002 Enterprise Edition	Two vulnerabilities exist: a buffer overflow vulnerability exists in the HTTP Receiver component due to a boundary error, which could let a remote malicious user cause a Denial or Service or execute arbitrary code (<i>Note: this vulnerability only affects BizTalk Server 2002</i>); and a vulnerability exists due to an input validation error in some of the pages used by the DTA (Document Tracking and Administration) web interface, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-016.asp	BizTalk Buffer Overflow & DTA Interface CVE Names: CAN-2003-0117, CAN-2003-0118	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. <i>Proofs of Concept exploits have been published.</i>
Microsoft ⁷⁴ <i>Exploit released</i> ⁷⁵	Windows 2000, XP	BizTalk Server 2000 Developer Edition, SP1a, SP2, 2000 Enterprise Edition, SP1a, SP2, 2000 Standard Edition, SP1a, SP2, 2002 Developer Edition, 2002 Enterprise Edition	Two vulnerabilities exist: a buffer overflow vulnerability exists in the HTTP Receiver component due to a boundary error, which could let a remote malicious user cause a Denial or Service or execute arbitrary code (<i>Note: this vulnerability only affects BizTalk Server 2002</i>); and a vulnerability exists due to an input validation error in some of the pages used by the DTA (Document Tracking and Administration) web interface, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-016.asp	BizTalk Buffer Overflow & DTA Interface CVE Names: CAN-2003-0117, CAN-2003-0118	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. <i>Proof of Concept exploit has been published.</i>
Microsoft ⁷⁶	Windows NT 4.0/2000, XP	IIS 4.0, 4.0 alpha, 5.0, 5.1,	An information disclosure vulnerability exists in the Authentication Manager, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Internet Information Server Authentication Manager	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft ⁷⁷	Windows	Internet Explorer 6.0 SP1	A Denial of Service vulnerability exists if a malicious user submits a DHTML page that contains a malformed 'AnchorClick' link.	No workaround or patch available at time of publishing.	Internet Explorer DHTML AnchorClick Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

⁷² Microsoft Security Bulletin, MS03-016, April 30, 2003.

⁷³ Bugtraq, May 5, 2003.

⁷⁴ Microsoft Security Bulletin, MS03-016, April 30, 2003.

⁷⁵ SecurityFocus, May 5, 2003.

⁷⁶ SecurityTracker Alert ID, 1006704, May 4, 2003.

⁷⁷ Bugtraq, May 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁸ <i>Microsoft issues bulletin⁷⁹</i> <i>Microsoft updates bulletin⁸⁰</i>	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, 2000 SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A remote Denial of Service vulnerability exists in the Remote Procedure Call (RPC) Service when a specifically malformed packet is sent to TCP port 135. <i>Bulletin updated to include information and link to Microsoft Knowledge Base Article 814119, for customers experiencing technical problems after installing this patch.</i>	<i>Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-010.asp</i>	Windows 2000 RPC Service Remote Denial of Service CVE Name: CAN-2002-1561	Low	Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.
Microsoft ⁸¹	Windows 98/ME/NT 4.0/XP	Windows Media Player XP, 7.1	A vulnerability exists in the way skin files are handled due to insufficient validation of URLs when initiating a download, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-017.asp	Windows Media Player Skin File Download CVE Name: CAN-2003-0228	High	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
Microsoft ⁸²	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&SP2, 6.0, 6.0 SP1	A zone bypass vulnerability exists when an attempt is made to open a page that contains numerous 'file://' requests, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Internet Explorer file:// Request Bypass	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

⁷⁸ Immunity Inc. Advisory, October 18, 2002.

⁷⁹ Microsoft Security Bulletin, MS03-010, March 26, 2003.

⁸⁰ Microsoft Security Bulletin, MS03-010 V1.1, May 13, 2003.

⁸¹ Microsoft Security Bulletin MS03-017, May 9, 2003.

⁸² Bugtraq, May 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁸³ <i>Microsoft updates bulletin</i> ⁸⁴	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, SP1-SP3, 5.5, 5.5 SP1&2, 6.0, SP1	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in 'URLMON.DLL' due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in 'plugin.ocx' due to insufficient checking of parameters, which could let a remote malicious user execute arbitrary script code. <i>Bulletin updated mitigating factors and Frequently Asked Questions to note that the URLMON.DLL buffer overflow vulnerability is not blocked from the HTML e-mail vector by the Outlook Email Security Update or the default settings of Outlook 2002 and Outlook Express 6.0.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-015.asp	Internet Explorer Multiple Vulnerabilities CVE Name: CAN-2003-0113, CAN-2003-0115	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁸³ Microsoft Security Bulletin, MS03-015, April 23, 2003.

⁸⁴ Microsoft Security Bulletin, MS03-015 V1.1 May 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mirabilis ⁸⁵	Windows 95/98/ME/NT 4.0/2000, XP	ICQ Pro 2003a & prior	Multiple vulnerabilities exist: a format string vulnerability exists in the POP3 Client's UIDL field due to a programming error when handling the unique ID of an e-mail message, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the POP3 client due to insufficient bounds checking when verifying the length of the date and subject e-mail header fields, which could let a malicious user execute arbitrary commands; a vulnerability exists in the "ICQ Features on Demand" due to hard-coded information and lack of authentication signatures, which could let a malicious user execute arbitrary code; a Denial of Service vulnerability when rendering HTML code within message window advertisements due to a lack of an authentication mechanism used while accepting advertisements; and a Denial of Service vulnerability exists when parsing GIF89a headers due to insufficient validation of GIF files.	No workaround or patch available at time of publishing.	Mirabilis ICQ Multiple Vulnerabilities CVE Names: CAN-2003-0235, CAN-2003-0236, CAN-2003-0237, CAN-2003-0238, CAN-2003-0239	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required for the Denial of Service vulnerability.

⁸⁵ Core Security Technologies Advisory, CORE-2003-0303, March 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MIT ^{86, 87, 88, 89, 90} <i>More upgrades issued⁹¹</i>	Unix	Kerberos 5 1.0, 1.0.6, 1.1, 1.1.1, 1.2-1.2.7, 1.3 -alpha1	Several vulnerabilities exist: a buffer overflow vulnerability exists in the principal names array, which could let a malicious user cause a Denial of Service and execution of arbitrary code depending upon the malloc implementation; and a buffer overflow vulnerability exists in the principal names array due to unexpected results when calculating static values with user-supplied values, which could let a malicious user execute arbitrary code.	<u>MIT:</u> http://web.mit.edu/kerberos/www/advisories/MITKRBS-SA-2003-005-patch.txt <u>RedHat:</u> ftp://updates.redhat.com/ <u>Debian:</u> http://security.debian.org/pool/updates/main/k/krb5/ <u>Mandrake:</u> http://www.mandrakesecurity.net/en/advisories/ <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/	Kerberos 5 Principal Name Buffer Overflows CVE Names: CAN-2003-0072, CAN-2003-0082	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Multiple Vendors ⁹² <i>New exploit script published⁹³</i> <i>Opera 7.11 also vulnerable⁹⁴</i>	Windows, Unix	IBM JDK 1.3.1; Sun JRE (Linux, Solaris, Windows Production Release) 1.3.1-1.3.1_07, 1.4-1.4.0_03, 1.4.1, 1.4.1_01, Sun SDK (Linux, Solaris, Windows Production Release) 1.3.1-1.3.1_07, 1.4-1.4.0_03, 1.4.1, 1.4.1_01 <i>Opera 7.11j</i>	A Denial of Service vulnerability exists in several java.util.zip implementations due to insufficient checks to see whether the parameters are NULL values.	Upgrade to Sun JDK 1.4.1_02 available at: http://java.sun.com/j2se/1.4/	Multiple Vendor Java Virtual Machine java.util.zip Null Value Denial of Service	Low	Bug discussed in newsgroups and websites. <i>Exploit script has been published.</i> <i>Another exploit script has been published.</i>

⁸⁶ MIT krb5 Security Advisory, 2003-005, March 20, 2003.

⁸⁷ Debian Security Advisory, DSA 266-1, March 24, 2003.

⁸⁸ Red Hat Security Advisory, RHSA-2003:051-01, March 26, 2003.

⁸⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:043, April 1, 2003.

⁹⁰ Red Hat Security Advisory, RHSA-2003:091-01, April 1, 2003.

⁹¹ Conectiva Linux Security Announcement, CLA-2003:639, May 5, 2003.

⁹² Bugtraq, March 14, 2003.

⁹³ Bugtraq, April 29, 2003.

⁹⁴ Bugtraq, May 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁹⁵	Unix	GNOME Balsa 2.0.6, 2.0.10; Mutt Mutt 1.2-1, 1.2.5, 1.3.12, 1.3.16, 1.3.17, 1.3.22, 1.3.24, 1.3.25, 1.3.27, 1.3.28, 1.4.0, 1.4.1; University of Washington Pine 4.30, 4.33, 4.44, 4.52, 4.53	Several buffer overflow vulnerabilities exist when an excessive value for the mailbox size is handled by the client, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	This issue has reportedly been addressed in University of Washington imap-2002c. Users should contact the vendor to obtain an upgraded version.	Multiple Vendor IMAP Client Mailbox Size	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Multiple Vendors ⁹⁶	Windows NT 4.0/2000, Unix	Borland/ Inprise Interbase 6.0; Firebird Firebird 1.0.2, 1.0.0	A buffer overflow vulnerability exists in the 'gds_inet_server,' 'gds_drop,' and 'gds_lock_mgr' binaries, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Firebird & Interbase Environment Variable Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Multiple Vendors ^{97, 98}	Unix	Linux kernel 2.4-2.4.20, 2.5.0-2.5.69	A vulnerability exists in the 'ioperm' system call due to insufficient permissions, which could let a malicious user obtain sensitive information.	RedHat: ftp://updates.redhat.com/ Engarde: http://www.linuxsecurity.com/advisories/engarde_advisory-3259.html	Linux Kernel IOPERM System Call Insufficient Permissions CVE Name: CAN-2003-0246	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

⁹⁵ Bugtraq, May 14, 2003.

⁹⁶ Dtors Security Research, May 9, 2003.

⁹⁷ Red Hat Security Advisory, RHSA-2003:172-00, May 14, 2003.

⁹⁸ Guardian Digital Security Advisory, ESA-20030515-017, May 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 99, 100, 101, 102</p> <p><i>More vendors release upgrades</i> 103, 104, 105, 106, 107</p> <p><i>More vendors release upgrades</i> 108, 109</p>	Unix	Linux kernel 2.2-2.2.24, 2.4-2.4.21 pre1	A vulnerability exists in the ptrace() system call due to a failure to restrict trace permissions on some root spawned processes, which could let a malicious user obtain root access.	<p>Upgrade available at: ftp://ftp.kernel.org/pub/linux/kernel/v2.2/linux-2.2.25.tar.gz</p> <p>RedHat: ftp://updates.redhat.com/</p> <p>Engarde: ftp://ftp.engardelinux.org/pub/engarde/stable/updates/</p> <p>Trustix: http://www.trustix.net/pub/Trustix/updates/</p> <p>Debian: http://security.debian.org/pool/updates/main/k/</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>SuSE: ftp://ftp.suse.com/pub/suse</p> <p>SCO: ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/</p> <p>Engarde: http://www.linuxsecurity.com/advisories/engarde_advisory-3259.html</p>	Linux Kernel Root Access	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.

⁹⁹ Red Hat Security Advisory, RHSA-2003:098-00, March 17, 2003.

¹⁰⁰ EnGarde Secure Linux Security Advisory, ESA-20030318-009, March 18, 2003.

¹⁰¹ Trustix Secure Linux Security Advisory, TSLSA-2003-0007, March 18, 2003.

¹⁰² Red Hat Security Advisory, RHSA-2003:088-01, March 19, 2003.

¹⁰³ SuSE Security Announcement, SuSE-SA:2003:021, March 25, 2003.

¹⁰⁴ Debian Security Advisory, DSA 270-1, March 27, 2003.

¹⁰⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:038, March 27, 2003.

¹⁰⁶ Mandrake Linux Security Update Advisory, MDKSA-2003:039, March 28, 2003.

¹⁰⁷ Debian Security Advisory, DSA 276-1, April 3, 2003.

¹⁰⁸ SCO Security Advisory, CSSA-2003-020.0, May 12, 2003.

¹⁰⁹ Guardian Digital Security Advisory, ESA-20030515-017, May 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 110, 111, 112, 113, 114, 115, 116</p> <p><i>Engarde updates bulletin</i>¹¹⁷</p>	Unix	<p>Todd Miller Sudo 1.5.9, 1.6-1.6.2, 1.6.3 p1-1.6.3 p7, 1.6.3, 1.6.4 p1-1.6.4 p2, 1.6.4, 1.6.5 p1-1.6.5 p2, 1.6.5</p>	<p>A vulnerability exists in the customized password prompt feature, which could let a malicious user obtain root privileges.</p> <p><i>Due to an error, this vulnerability was never fixed in later EnGarde versions.</i></p>	<p>Todd Miller: ftp://ftp.sudo.ws/pub/sudo/sudo-1.6.6.tar.gz</p> <p>RedHat: ftp://updates.redhat.com/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Debian: http://security.debian.org/dists/stable/updates/main/</p> <p>Mandrake: http://www.mandrakesecurity.net/en/ftp.php</p> <p>Engarde: http://ftp.engardelinux.org/pub/engarde/stable/updates/</p> <p>Trustix: http://www.trustix.net/pub/Trustix/updates/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/i386/update/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p>	<p>Sudo Password Prompt Heap Overflow</p> <p>CVE Name: CAN-2002-0184</p>	High	Bug discussed in newsgroups and websites.

¹¹⁰ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:072-07, April 25, 2002.

¹¹¹ Conectiva Linux Security Announcement, CLA-2002:475, April 26, 2002.

¹¹² Debian Security Advisory, DSA-128-1, April 26, 2002.

¹¹³ Mandrake Linux Security Update Advisory, MDKSA-2002:028, April 26, 2002.

¹¹⁴ EnGarde Secure Linux Security Advisory, ESA-20020429-010, April 29, 2002.

¹¹⁵ Trustix Secure Linux Security Advisory, TSLSA-2002-0046, April 29, 2002.

¹¹⁶ SuSE Security Announcement, SuSE-SA:2002:014, April 30, 2002.

¹¹⁷ Guardian Digital Security Advisory, ESA-20030515-015, May 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 118, 119, 120, 121, 122, 123, 124</p> <p><i>More upgrades released</i> 125, 126</p>	<p>MacOS 10.2- 10.2.4; Unix</p>	<p>Compaq Tru64 4.0x, 5.0x; HP HP9000 servers running CIFS/9000 Server versions through A.01.09.02 on HP-UX 11.0, 11.11(11i), and 11.22; Samba Samba 2.0.0-2.0.10, 2.2.0, 2.2.0a, 2.2.1 a, 2.2.3 a-2.2.8, Samba-TNG 0.3, 0.3.1; Sun Solaris 2.5.1, 2.5.1_ppc, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86, Update 2</p>	<p>Multiple remote buffer overflow vulnerabilities exist, which could let a remote malicious user execute arbitrary code with root privileges.</p>	<p>Debian: http://security.debian.org/pool/updates/main/s/samba/ Immunix: http://download.immunix.org/ImmunixOS Samba: http://us1.samba.org/samba/ftp/samba-2.2.8a.tar.gz Slackware: ftp://ftp.slackware.com/pub/slackware/ OpenPKG: ftp://ftp.openpkg.org/release Mandrake: http://www.mandrakesecure.net/en/ftp.php FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/ RedHat: ftp://updates.redhat.com/</p> <p>SCO: ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1 Sun Microsystems: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert%2F53924</p>	<p>Multiple Vendor Samba Unspecified Remote Buffer Overflows</p> <p>CVE Name: CAN-2003-0196</p>	<p>High</p>	<p>Bug discussed in newsgroups and websites.</p> <p>Vulnerability has appeared in the press and other public media.</p>

¹¹⁸ Debian Security Advisory, DSA 280-1, April 7, 2003.

¹¹⁹ FreeBSD Security Advisory, FreeBSD-SN-03:01, April 7, 2003.

¹²⁰ Immunix Secured OS Security Advisory, IMNX-2003-7+-006-01, April 7, 2003.

¹²¹ Mandrake Linux Security Update Advisory, MDKSA-2003:044, April 7, 2003.

¹²² OpenPKG Security Advisory, OpenPKG-SA-2003.028, April 7, 2003.

¹²³ Red Hat Security Advisory, RHSA-2003:137-02, April 9, 2003.

¹²⁴ Hewlett-Packard Company Security Bulletin, HPSBUX0304-254, April 9, 2003.

¹²⁵ SCO Security Advisory, CSSA-2003-017.0, May 2, 2003.

¹²⁶ Sun(sm) Alert Notification, 53924, May 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 127, 128, 129, 130, 131, 132, 133, 134</p> <p><i>SCO releases upgrade 135</i></p>	<p>MacOS X 10.0.4, 10.2x, Unix</p>	<p>HP CIFS/9000 Server A.01.09.01, A.01.09, A.01.08.01, A.01.08, A.01.07, A.01.06, A.01.05; Samba Samba 2.0.0- 2.0.10, 2.2.0, 2.2.0a, 2.2.0, 2.2.2-2.2.7</p>	<p>A buffer overflow vulnerability exists in the Samba main smbd code, which could let a remote malicious user execute arbitrary code with root privileges; and a race condition vulnerability exists when writing to reg files, which could let a malicious user obtain elevated privileges.</p>	<p>Samba: http://download.samba.org/samba/ftp/ HP Hotfix: ftp://samba:samba@hprc.external.hp.com/ SuSE: ftp://ftp.suse.com/pub/suse/ OpenPKG: ftp://ftp.openpkg.org/release Mandrake: http://www.mandrakesecurity.net/en/ftp.php RedHat: ftp://updates.redhat.com/ SGI: http://freeware.sgi.com/beta/fw_samba-2.2.8.tardist Debian: http://security.debian.org/pool/updates/main/s/samba/ Trustix: http://www.trustix.net/pub/Trustix/updates/</p> <p>SCO: ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/</p>	<p>Samba SMB/CIFS Buffer Overflow & Reg File Race Condition</p> <p>CVE Names: CAN-2003-0085, CAN-2003-0086</p>	<p>Medium/High</p> <p>(High if arbitrary code can be executed)</p>	<p>Bug discussed in newsgroups and websites.</p> <p>There is no exploit code required for the race condition vulnerability.</p> <p>Vulnerability has appeared in the press and other public media.</p>

¹²⁷ Debian Security Advisory, DSA-262-1, March 15, 2003.

¹²⁸ Mandrake Linux Security Update Advisory, MDKSA-2003:032, March 15, 2003.

¹²⁹ Red Hat Security Advisory, RHSA-2003:095-01, March 17, 2003.

¹³⁰ Hewlett-Packard Company Security Bulletin, HPSBUX0303-251, March 18, 2003.

¹³¹ OpenPKG Security Advisory, OpenPKG-SA-2003.021, March 18 2003.

¹³² Trustix Secure Linux Security Advisory, TSLSA-2003-0011, March 18, 2003.

¹³³ SGI Security Advisory, 20030302-01-I, March 19, 2003.

¹³⁴ SuSE Security Announcement, SuSE-SA:2003:015, March 19, 2003.

¹³⁵ SCO Security Advisory, CSSA-2003-017.0, May 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147</p> <p><i>More upgrades released 148, 149</i></p>	MacOS 10.2- 10.2.4; Unix	<p>MacOS X 10.2- 10.2.4;</p> <p>Compaq Tru64 4.0x, 5.0x;</p> <p>HP HP9000 servers running CIFS/9000 Server versions through A.01.09.02 on HP-UX 11.0, 11.11(11i), and 11.22;</p> <p>Samba 2.0.0- 2.0.10, 2.2.0, 2.2.0a, 2.2.1 a, 2.2.3 a- 2.2.8,</p> <p>Samba-TNG 0.3, 0.3.1;</p> <p>Sun Solaris 2.5.1, 2.5.1_ppc, 2.5.1_x86, 2.6, 2.6_x86, 7.0-9.0, 7.0_x86- 9.0_x86, Update 2</p>	A buffer overflow vulnerability exists for Samba in the 'call_trans2open' function when user-supplied data is copied into a static buffer, which could let a remote malicious user obtain root access and execute arbitrary commands.	<p>Apple: http://docs.info.apple.com/article.html?artnum=120211</p> <p>Debian: http://security.debian.org/pool/updates/main/s/samba/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br</p> <p>Immunix: http://download.immunix.org/ImmunixOS</p> <p>Samba: http://us1.samba.org/samba/ftp/samba-2.2.8a.tar.gz</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>OpenPKG: ftp://ftp.openpkg.org/release</p> <p>Mandrake: http://www.mandrakesecurity.net/en/ftp.php</p> <p>Trustix: http://www.trustix.net/pub/Trustix/updates/</p> <p>SGI: ftp://patches.sgi.com/support/free/security/patches/</p> <p>FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/</p> <p>RedHat: ftp://updates.redhat.com/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse</p> <p>SCO: ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/</p> <p>Sun Microsystems: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert%2F53924</p>	Multiple Vendors 'call_trans2open' Remote Buffer Overflow	High	<p>Bug discussed in newsgroups and websites. Exploit scripts have been published.</p> <p>Vulnerability has appeared in the press and other public media.</p>

¹³⁶ Debian Security Advisory, DSA 280-1, April 7, 2003.

¹³⁷ FreeBSD Security Advisory, FreeBSD-SN-03:01, April 7, 2003.

¹³⁸ Immunix Secured OS Security Advisory, IMNX-2003-7+-006-01, April 7, 2003.

¹³⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:044, April 7, 2003.

¹⁴⁰ SuSE Security Announcement, SuSE-SA:2003:025, April 7, 2003.

¹⁴¹ OpenPKG Security Advisory, OpenPKG-SA-2003.028, April 7, 2003.

¹⁴² Trustix Secure Linux Security Advisory, TSLSA-2003-0019, April 8, 2003.

¹⁴³ Conectiva Linux Security Announcement, CLA-2003:624, April 8, 2003.

¹⁴⁴ Red Hat Security Advisory, RHSA-2003:137-02, April 9, 2003.

¹⁴⁵ SGI Security Advisory, 20030403-01-P, April 9, 2003.

¹⁴⁶ Hewlett-Packard Company Security Bulletin, HPSBUX0304-254, April 9, 2003.

¹⁴⁷ Apple Security Update, 61798, April 10, 2003.

¹⁴⁸ SCO Security Advisory, CSSA-2003-017.0, May 2, 2003.

¹⁴⁹ Sun(sm) Alert Notification, 53924, May 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mutt ^{150, 151} <i>Debian releases another advisory</i> ¹⁵²	Unix	Mutt 1.3.12, 1.3.12-1, 1.3.16, 1.3.17, 1.3.22, 1.3.24, 1.3.25, 1.3.27, 1.3.28	A buffer overflow vulnerability exists due to insufficient verification of folder names, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	<u>Debian:</u> http://security.debian.org/pool/updates/main/m/mutt	Mutt IMAP Remote Folder Buffer Overflow CVE Name: CAN-2003-0167	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
MySQL AB ^{153, 154, 155, 156, 157, 158, 159, 160, 161} <i>More advisories issued</i> ^{162, 163}	Unix	MySQL 3.20.32 a, 3.22.26- 3.22.30, 3.22.32, 3.23.2- 3.23.5, 3.23.8- 3.23.10, 3.23.23- 3.23.31, 3.23.33, 3.23.34, 3.23.36- 3.23.53, 4.0.0-4.0.3, 4.0.5 a	Several vulnerabilities exist: a vulnerability exists in the password authentication mechanism, which could let a malicious user obtain unauthorized database access; a vulnerability exists in the COM_CHANGE_USER command due to insufficient bounds checking, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the read_rows function because stored row sizes are not verified by the client, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. <i>A vulnerability also exists when COM_TABLE_DUMP malformed commands are issued, which could let a malicious user cause a Denial of Service.</i> <i>NOTE: The updates provided in the EnGarde Advisory, ESA-20021213-033 missed one critical fix for the COM_TABLE_DUMP vulnerability.</i>	<u>Debian:</u> http://security.debian.org/pool/updates/main/m/mysql/ <u>MySQL:</u> http://www.mysql.com/downloads/mysql-3.23.html <u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php <u>SuSE:</u> ftp://ftp.suse.com/pub/suse/ <u>EnGarde:</u> ftp://ftp.engardelinux.org/pub/engarde/stable/updates <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/ <u>Trustix:</u> ftp://ftp.trustix.net/pub/Trustix/updates/ <u>RedHat:</u> ftp://updates.redhat.com	MySQL Multiple Vulnerabilities CVE Names: CAN-2002-1373, CAN-2002-1374, CAN-2002-1375, CAN-2002-1376	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

¹⁵⁰ SuSE Security Announcement, SuSE-SA:2003:020, March 24, 2003.

¹⁵¹ Debian Security Advisory, DSA 268-1, March 25, 2003.

¹⁵² Debian Security Advisory, DSA 300-1, May 6, 2003.

¹⁵³ e-matters GmbH Security Advisory, December 12, 2002.

¹⁵⁴ EnGarde Secure Linux Security Advisory, ESA-20021213-033, December 13, 2002.

¹⁵⁵ OpenPKG Security Advisory, OpenPKG-SA-2002.013, December 16, 2002.

¹⁵⁶ Gentoo Linux Security Announcement, 200212-2.1, December 16, 2002.

¹⁵⁷ Debian Security Advisory, DSA-212-1, December 17, 2002.

¹⁵⁸ Conectiva Linux Security Announcement, CLA-2002:555, December 17, 2002.

¹⁵⁹ Mandrake Linux Security Update Advisory, MDKSA-2002:087, December 18, 2002.

¹⁶⁰ Trustix Secure Linux Security Advisory #2002-0086, TSLSA-2002-0086, December 19, 2002.

¹⁶¹ SuSE Security Announcement, SuSE-SA:2003:003, January 2, 2003.

¹⁶² Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:288-22, January 15, 2003.

¹⁶³ EnGarde Secure Linux Security Advisory, ESA-20030127-001, January 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL ¹⁶⁴	Unix	MySQL 4.x, 3.x	A vulnerability exists due to a weak password encryption algorithm, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MySQL Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Neoteris.com ¹⁶⁵	Multiple	Instant Virtual Extranet 3.01	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of an argument that is passed to an IVE CGI script, which could let a remote malicious user hijack valid sessions.	Patch available at: https://support.neoteris.com	Instant Virtual Extranet Cross-Site Scripting CVE Name: CAN-2003-0217	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Netscape ¹⁶⁶	Multiple	Navigator 7.0 2	A vulnerability exists due to the way the 'historyback()' function is handled, which could result in a false sense of security.	No workaround or patch available at time of publishing.	Navigator historyback() Function	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Novell ¹⁶⁷	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	NetMail 3.10-3.10d	Multiple vulnerabilities exist which could let a malicious user cause a Denial of Service. For more information, see Technical Information Document at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2965676.htm .	Patches available at: http://support.novell.com/servelet/filedownload/pub/netmail310e.zip	NetMail Multiple Vulnerabilities	Low	Bug discussed in newsgroups and websites.
OpenSSH ¹⁶⁸	Unix	OpenSSH 3.4 p1, 3.6.1 p1	A vulnerability exists in OpenSSH when using Pluggable Authentication Modules (PAM) because analysis of the response time during authentication will let a remote malicious user obtain sensitive information.	Upgrade available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-3.6.1p2.tar.gz	OpenSSH-portable Enabled PAM Delay Information Disclosure CVE Name: CAN-2003-0190	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
OpenSSH ¹⁶⁹	MacOS X 10.x, Unix	OpenSSH 3.1 p1, 3.2, 3.2.2 p1, 3.2.3 p1, 3.3 p1, 3.3, 3.4 p1, 3.4, 3.5, 3.6.1p2, 3.6.1 p1, 3.6.1	A timing leak vulnerability exists, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	OpenSSH Remote Root Authentication Timing Side-Channel	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁶⁴ Secunia Security Advisory, May 9, 2003.

¹⁶⁵ Bugtraq, May 12, 2003.

¹⁶⁶ SecurityFocus, May 13, 2003.

¹⁶⁷ SecurityFocus, May 6, 2003.

¹⁶⁸ Mediaservice.net Security Advisory, April 30, 2003.

¹⁶⁹ SecurityFocus, May 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software ¹⁷⁰ <i>Upgrade now available</i> ¹⁷¹	Windows 95/98/ME/NT 4.0/2000, XP	Opera Web Browser 6.0 win32-6.0.5 win32, 7.0 win3- 7.0 3win32, 7.10	A vulnerability exists due to insufficient bounds checking on filename extensions, which could let a remote malicious user cause a Denial of Service.	<i>Upgrade now available:</i> http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows	Opera 6/7 Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Owl ¹⁷²	Windows, Unix	Owl Intranet Engine 0.7	A vulnerability exists in the 'browse.php' script due to insufficient sanitization when checking the validity of usernames and passwords, which could let a malicious user bypass authentication mechanisms.	No workaround or patch available at time of publishing.	Owl Intranet Engine Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Palm, Inc. ¹⁷³	Multiple	Palm OS 3.3, 3.5 h, 3.5.2, 4.0, 4.1	A remote Denial of Service vulnerability exists when a malicious user floods the system with ICMP ECHO_REQUEST traffic.	No workaround or patch available at time of publishing.	PalmOS Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Phorum ¹⁷⁴	Windows, Unix	Phorum 3.4-3.4.2	A vulnerability exists in the 'subject,' 'author's name,' and 'author's e-mail' fields due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: http://phorum.org/downloads/phorum-3.4.3.tar.gz	Phorum Message Form Field HTML Injection Variant	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁷⁰ Bugtraq, April 28, 2003.

¹⁷¹ SecurityFocus, May 12, 2003.

¹⁷² SecurityFocus, May 14, 2003.

¹⁷³ Bugtraq, May 14, 2003.

¹⁷⁴ Bugtraq, May 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Phorum ¹⁷⁵	Windows, Unix	Phorum 3.4-3.4.2	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information; multiple path disclosure vulnerabilities exist because the path to the webroot is disclosed when certain scripts are called incorrectly, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists in the 'Register.php,' 'post.php,' 'Common.php,' and 'login.php' scripts due to insufficient sanitization of user-supplied URI parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the 'Phorum Edit user' profile page due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'UserAdmin' page due to insufficient sanitization of user-supplied URL data, which could let a remote malicious user execute arbitrary code; a vulnerability exists in 'Phorum Stats' program due to insufficient sanitization of user-supplied URL data, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'Register.php,' and 'login.php' scripts because the script can be used to anonymously launch attacks on other sites in the context of the website.	Upgrade available at: http://phorum.org/downloads/phorum-3.4.3.tar.gz	Phorum Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Directory Traversal vulnerability can be exploited via a web browser.

¹⁷⁵ Secunia Security Advisory, May 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP Outsourcing ¹⁷⁶	Windows, Unix	IdeaBox 1.0	A vulnerability exists in the 'include.php' script and 'ideaDir' variable due to insufficient validation of user-supplied variables, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	IdeaBox Remote Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Pi3 ¹⁷⁷	Unix	Pi3Web 1.0.3, 2.0, 2.0.1	A Denial of Service vulnerability exists when a malicious GET request is submitted to the server.	No workaround or patch available at time of publishing.	Pi3Web Malformed GET Request Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PoPToP Development Team ¹⁷⁸	Unix	PPTP Server 1.1.4 – b1-b3	A buffer overflow vulnerability exists in the 'sprintf()' function due to insufficient bounds checking, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://sourceforge.net/projects/showfiles.php?group_id=44827	PPTP BCRELAY sprintf() Buffer Overflow	High	Bug discussed in newsgroups and websites.
Ralf Hoffmann ¹⁷⁹	Unix	Worker filemanager 2.7 & prior	A vulnerability exists in the X-Window file manager, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.boomerangsworld.de/worker/downloads/worker-2.7.1.tar.bz2	Filemanager Directory Creation Race Condition	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Roberto Beltrame ¹⁸⁰	Windows, Unix	PHP-Proxima	A vulnerability exists in the 'autohtml.php' script due to insufficient verification of user-supplied variables, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP-Proxima 'autohtml.php' Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Siemens Communications ¹⁸¹	Multiple	Siemens Mobile Phones M45, S45	A remote Denial of Service vulnerability exists when handling malformed image attachments in SMS messages.	No workaround or patch available at time of publishing.	Siemens Malformed Image Attachment Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Six Apart ¹⁸²	Windows, Unix	Movable Type 2.0	A vulnerability exists due to insufficient sanitization of encoded character HTML tags, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.movabletype.org/download.shtml	Movable Type Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁷⁶ Secunia Security Advisory, April 30, 2003.

¹⁷⁷ Rosiello Security Advisory, May 12, 2003.

¹⁷⁸ SecurityFocus, May 13, 2003.

¹⁷⁹ SecurityTracker Alert ID, 1006702, May 3, 2003.

¹⁸⁰ Bugtraq, May 14, 2003.

¹⁸¹ Bugtraq, May 6, 2003.

¹⁸² SecurityTracker Alert ID, 1006770, May 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
slocate ^{183, 184} <i>Conectiva releases upgrade 185</i>	Unix	slocate 2.6	A buffer overflow vulnerability exists when the slocate program is run with command line arguments of excessive length, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.geekreview.com/slocate/src/slocate-2.7.tar.gz Mandrake: http://www.mandrakesecurity.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/s/slocate/ SCO: ftp://ftp.sco.com/pub/updates/OpenLinux/ Conectiva: ftp://atualizacoes.conectiva.com.br/	slocate Buffer Overrun	High	Bug discussed in newsgroups and websites. Exploit has been published.
Snitz Forums 2000 ¹⁸⁶	Windows	Snitz Forums 2000 3.3.03	A vulnerability exists in the 'register.asp' script due to insufficient checking of user-supplied input, which could let a remote malicious user execute arbitrary commands.	Patch available at: http://prdownloads.sourceforge.net/sourceforge/sf2k/sf2k_v34_03.zip	Snitz Forums 2000 'Register.ASP' Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Splatt.it ¹⁸⁷	Windows, Unix	Splatt Forum 4.0	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'Search' function due to insufficient filtering of user-supplied URI parameters, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability exists when messages are posted because special characters are not stripped from the message, which could let a remote malicious user execute arbitrary HTML and script code.	Patch available at: http://www.splatt.it/modules.php?name=Downloads&do=viewdownload&details&lid=166&title=Splatt%20Forum%204.0%20Fix%201	Splatt Forum Module Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proofs of exploit have been published.
Stalker Software, Inc. ¹⁸⁸	Unix	CommuniGate Pro 3.1, 3.2 b7, 3.2 b5, 3.2.4, 3.3b2, 3.3b1, 3.3.2, 3.4b3, 4.0b3, 4.0b2, 4.0.1, 4.0.2, 4.0.3, 4.0.6	A vulnerability exists in the Webmail interface because an authenticated user's Session ID value is exposed via the HTTP Referer field when downloading images, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.stalker.com/download.html	CommuniGate Pro Webmail Session Hijacking	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁸³ USG Security Advisory, USG-SA-2003.001, January 24, 2003.

¹⁸⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:015, February 5, 2003.

¹⁸⁵ Conectiva Linux Security Announcement, CLA-2003:643, May 8, 2003.

¹⁸⁶ SecurityFocus, May 10, 2003.

¹⁸⁷ Frame4 Security Advisory, FSA-2003:001, May 1, 2003.

¹⁸⁸ Bugtraq, May 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems ¹⁸⁹	Windows, NT 4.0/2000, Unix	Sun ONE Directory Server 5.1, SP1, 5.0, SP1&SP2, 4.16, SP1,	A buffer overflow vulnerability exists in the 'ns-slapd' service, which could let a local/remote malicious user cause a Denial of Service.	Patches available at: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=113859&rev=01	Sun ONE Directory Server Denial Of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc. ¹⁹⁰	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A remote Denial of Service vulnerability exists in rpcbind(1M) which will block traffic to all RPC services on the vulnerable system.	Patches available at: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=105402&rev=42	Solaris RPCbind Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Verilink ¹⁹¹	Multiple	NetEngine 6100-4	A remote Denial of Service vulnerability exists due to the way TFTP packets are handled.	No workaround or patch available at time of publishing.	NetEngine Broadband Router TFTP Packet Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
VIM Development Group ¹⁹² <i>Mandrake releases patch¹⁹³</i> <i>Sun releases upgrade¹⁹⁴</i>	Unix	VIM 5.0-5.8, 6.0, 6.1	A vulnerability exists in the modelines function due to insufficient handling of input, which could let a remote malicious user execute arbitrary code. <i>Note: A conceptual worm has been reported that explicitly illustrates how this vulnerability could be further exploited to act as a mass mailing worm.</i>	<u>RedHat:</u> ftp://updates.redhat.com/ <u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php <u>Sun:</u> http://ftp.cobalt.sun.com/pub/packages/	VIM ModeLines Arbitrary Command Execution CVE Name: CAN-2002-1377	High	Bug discussed in newsgroups and websites. VIM Worm has been published that exploits this vulnerability.
X2 Studios, Ltd. ¹⁹⁵	Unix	XMMS Remote 0.1	An input validation vulnerability exists in the 'XMMS.pm' script, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://www.x2studios.com/download.php?id=9	XMMS Remote Arbitrary Command Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Young ZSoft ¹⁹⁶	Windows NT 4.0/2000, XP	CMail Server 4.0.2003.03 .27, 4.0.2002.11 .24	Several buffer overflow vulnerabilities exist when parsing e-mail headers due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.	Users are advised to contact the vendor for upgrade information.	CMailServer E-Mail Headers Buffer Overflows	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁸⁹ Sun(sm) Alert Notification, 52102, April 30, 2003.

¹⁹⁰ Sun(sm) Alert Notification, 50922, April 28, 2003.

¹⁹¹ SecurityTracker Alert ID, 1006723, May 8, 2003.

¹⁹² Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:297-17, January 16, 2003.

¹⁹³ Mandrake Linux Security Update Advisory, MDKSA-2003:012, February 3, 2003.

¹⁹⁴ Secunia Security Advisory, May 13, 2003.

¹⁹⁵ Secunia Security Advisory, May 13, 2003.

¹⁹⁶ Securiteam, May 12, 2003.

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

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

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

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

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 30 and May 14, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 41 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 14, 2003	PalmDoS.c	Script that exploits the PalmOS Remote Denial of Service vulnerability.
May 14, 2003	pi3web-DoS.c	Script that exploits the Pi3Web Malformed GET Request Denial of Service vulnerability.
May 14, 2003	vBulletin-preview-poc.html.txt	Exploit for the vBulletin Private Message vulnerability.
May 13, 2003	priv8cdr.pl	Local root exploit for the CDRRecord 'printf-like' Format String vulnerability.
May 12, 2003	CMailServer-exp.pl	Perl script that exploits the CMailServer E-Mail Headers Buffer Overflows vulnerability.
May 12, 2003	eserv-dos.pl	Perl script that exploits the EServ Remote Denial of Service vulnerability.
May 12, 2003	katax.c	Script that exploits the Leksbot KATAXWR binary vulnerability.
May 11, 2003	dsr-adv001.txt	Two local root exploit scripts for the Firebird GDS_Inet_Server Interbase Environment Variable Buffer Overflow vulnerability.
May 11, 2003	snuffi-0.1.tar.gz	A Linux kernel module that adds a hook to the incoming and outgoing queue of netfilter.
May 10, 2003	jelmer.zip	Exploit for the UnZip Directory Traversal vulnerability.
May 10, 2003	lotus-agent.java	Exploit for the Multiple Vendor Java Virtual Machine java.util.zip Null Value Denial of Service vulnerability.
May 10, 2003	snitz_exec.pl	Perl script that exploits the Splatt Forum Module Cross-Site Scripting vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 9, 2003	DSR-firebird.c	Script that exploits the Firebird GDS_Inet_Server Interbase Environment Variable Buffer Overflow vulnerability.
May 9, 2003	DSR-olbird.c	Script that exploits the Firebird GDS_Inet_Server Interbase Environment Variable Buffer Overflow vulnerability.
May 9, 2003	MediaPlayerExploit.java	Exploit for the Windows Media Player Skin File Download vulnerability.
May 9, 2003	mysqlfast.c	Exploit for the MySQL Weak Password Encryption vulnerability.
May 8, 2003	amap-2.1.tar.gz	A scanning tool that allows you to identify the applications that are running on a specific port by connecting to the port(s) and sending trigger packets
May 8, 2003	dmz.rar	Exploit for the Internet Explorer file:// Request Bypass vulnerability.
May 8, 2003	DSR-ltrisp.pl	Perl script that exploits the LTris Local Memory Corruption vulnerability.
May 8, 2003	ethereal-0.9.12.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
May 8, 2003	flashfxp_decrypt.c	Script that exploits the FlashFXP User Password Encryption vulnerability.
May 8, 2003	gossh.sh	A user identification remote exploit shell script that tells you whether or not a user exists by using a timing attack.
May 8, 2003	List-Proc-catmail.pl	Perl script that exploits the ListProc ULISTPROC_UMASK Buffer Overflow vulnerability.
May 8, 2003	nessus-2.0.5.tar.gz	A free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over a thousand remote security checks.
May 8, 2003	nmap-3.27.tgz	A utility for port scanning large networks, although it works fine for single hosts.
May 8, 2003	PFEexploit.c	Script that exploits the Personal Firewall Remote Authentication Buffer Overflow vulnerability.
May 8, 2003	rk.zip	Exploit for the NetEngine Broadband Router TFTP Packet Remote Denial of Service vulnerability.
May 7, 2003	disco-1.0.tar.gz	A passive IP discovery utility designed to sit on segments distributed throughout a network and discover unique IPs. In addition to IP discovery Disco has the ability to passively fingerprint TCP SYN packets to determine the host operating system.
May 7, 2003	DSR-youbin.pl	Local root exploit for the Youbin HOME Buffer Overflow vulnerability.
May 7, 2003	DSR-youbin.txt	Exploit for the Youbin HOME Buffer Overflow vulnerability.
May 7, 2003	eth0sniff.c.gz	A simple and versatile sniffer utility to monitor ports 21 (FTP) and 110 (POP) for quick accumulation of user and password strings.
May 7, 2003	ettercap-0.6.a.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
May 7, 2003	kerio.c	Script that exploits the Personal Firewall Remote Authentication Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 7, 2003	smtpscan-0.5.tar.gz	A tool to guess which MTA is used by sending several "special" SMTP requests and by comparing error codes returned with those in the fingerprint database.
May 6, 2003	splloit.pl	Perl script that exploits the FTGate PRO Multiple Buffer Overflows vulnerabilities.
May 4, 2003	ms-iis-bruteforce.pl	Perl script that exploits the Internet Information Server Authentication Manager vulnerability.
May 4, 2003	ms-iis-disc.pl	Perl script that exploits the Internet Information Server Authentication Manager vulnerability.
May 4, 2003	shj.pl	Perl script that exploits the CommuniGate Pro Webmail Session Hijacking vulnerability.
April 30, 2003	gossh.sh	Script that exploits the OpenSSH-portable Enabled PAM Delay Information Disclosure vulnerability.
April 30, 2003	ssh_brute.c	Script that exploits the OpenSSH-portable Enabled PAM Delay Information Disclosure vulnerability.
April 30, 2003	ws360_exp.c	Script that exploits the Web Server 4D HTTP Command Remote Buffer Overflow vulnerability.

Trends

- **Sobig.B (Aliases: Palyh or Mankx) infections have been reported from over 80 countries worldwide. This worm is spreading at an increasing pace. The largest infections seem to be in UK and USA. It spreads via e-mail attachments and Windows network shares. The e-mails sent by the worm pretend to come from support@microsoft.com and they contain the message text "All information is in the attached file." Windows users everywhere are urged to update their anti-virus definitions. For more information, see "Virus Section."**
- According to new research, nearly three-quarters of malicious connections to wireless networks are used for sending spam. A survey found that almost a quarter of unauthorized connections to the wireless LANs were intentional, and 71 per cent of those were used to send e-mails.
- **The Department of Homeland Security (DHS), Information Analysis and Infrastructure Protection (IAIP) has issued an advisory to heighten awareness of a recently discovered Snort(TM) vulnerability, a heap overflow in the Snort "stream4" preprocessor (CAN-2003-0029). For more information see 'Bugs, Holes, & Patches Table (CyberNotes 2003-08) and DHS/IAIP Advisory 03-018, located at: <http://www.nipc.gov/warnings/advisories/2003/03-018.htm>**
- **The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. The increase in events, which can include minor probes for holes in network security as well as major attacks, stems mainly from an increase in worms and automated attack software.**
- Over the past few weeks, there have been an increased number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. For more information, see CERT® Advisory CA-2003-08, located at: <http://www.cert.org/advisories/CA-2003-08.html>.

Viruses

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

W32.Fakelove (File Appender Virus): This is a file-appender virus that infects Portable Executable (PE) files. If a file infected with W32.Fakelove is executed, it creates two threads to infect all PE files whose extensions contain ".e" in drives C through Z and all shared folders. If the system date is the 1st of any month, the payload is triggered. It displays a message and attempts to delete all files found. The virus also transfers control back to the original host program.

W32/Fizzer-A (Aliases: I-Worm.Fizzer, W32/Fizzer.gen@MM, W32.HLLW.Fizzer@mm, WORM_FIZZER.A, W32/Fizzer@MM, Win32.Fizzer, Fizzer, Win32/Fizzer.A@mm) (Win32 Worm): This worm has been reported in the wild. It is a worm with IRC backdoor Trojan functionality. The worm spreads by file sharing on KaZaA shared networks and by e-mailing itself to contacts in the Microsoft Outlook and Windows address books and also to random e-mail addresses at the following domains:

- msn.com
- hotmail.com
- yahoo.com
- aol.com
- earthlink.net
- gte.net
- junocom.com
- netzero.com

The e-mail subject line, message text and attachment name are randomly constructed using long lists of strings. The worm may spoof the From: field of e-mails, replacing the sender's address with a randomly chosen name. Attachment names have an extension of EXE, COM, PIF, or SCR and may be combined with INI to give a double extension of INI.EXE, INI.COM, INI.PIF or INI.SCR. When run, W32/Fizzer-A drops the following files to the Windows folder:

- initbak.dat
- iservc.dll
- iservc.exe
- ProgOp.exe

and creates the registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SystemInit = %WINDOWS%\iservc.exe
- HKCR\txtfile\shell\open\command = %WINDOWS%\ProgOp.exe 0 7 '%1'

so that iservc.exe is run automatically each time the computer is restarted and ProgOp.exe is run whenever a file with an extension of TXT is opened. ProgOp.exe launches iservc.exe and then the default text editor. Iservc.exe connects to a remote IRC server, joins a specific channel, and then runs continuously in the background listening for commands being sent to the channel. A remote intruder will then be able to gain access and control over the computer using a regular IRC client. The remote intruder will be able to carry out a variety of actions, including a Denial-of-Service flooder attack. Iservc.dll is a keylogger component that may be used to log user keystrokes to the log file iservc.klg. W32/Fizzer-A provides similar access and control via AOL Instant Messenger channels by logging onto a remote AOL chat server using a random username. The worm attempts to spread via file sharing on P2P networks by copying itself to the KaZaA shared folder. W32/Fizzer-A attempts to terminate processes whose names contain any of various strings.

W32.HLLW.Kazping (Win32 Worm): This is a worm that attempts to spread itself through the KaZaA file-sharing network. It is written in the Microsoft Visual Basic programming language.

W32/Kickin-A (Aliases: W32/Kickin@MM, I-Worm.Cydog.c, WORM_CYDOG.C, W32.HLLW.Cydog.C@mm, Win32.Kickin.A, W32.HLLW.Kickin.A@mm) (Win32 Worm): This is a worm that will send itself to addresses found from a variety of sources including the Windows address book and HTML and XML files. It is intended to arrive in an e-mail with various sets of characteristics. The worm copies itself to folders shared by the peer-to-peer applications using various filenames.

W32/Kickin-A will create the following registry entries:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\System = <Current drive>:\<SystemFolder>\Kernel32.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunCyberWolf = <Current drive>:\<WindowsFolder>\CyberWolf.exe Windows Kernel = <Current drive>:\<SystemFolder>\Kernel32.exe

and will modify the following entries:

- HKCR\exefile\shell\open\command = <Current drive>:\<SystemFolder>\Kernel32.exe %1

W32/Kickin-A will attempt to open up Internet Explorer every 5 minutes to one of the following URLs:

- www.indiansnakes.cjb.net
- www.christinaaguilera
- www.brain-hack.com

W32/Kickin-A will create the file Script.ini. Script.ini is a mIRC script that will send a copy of W32/Kickin-A to other mIRC users. W32/Kickin-A will create the files Windows.lOg and CyberWolf.TxT. The worm will also attempt to shutdown certain anti-virus software.

W32/Lovgate-I (Win32 Worm): This worm has been reported in the wild. It is a minor variant of W32/Lovgate-J.

W32/Lovgate-J (Aliases: PE_LOVGATE.K, Win32/Lovgate.J, W32.HLLW.Lovgate.H@mm, WORM_LOVGATE.K, W32/Lovgate.k@MM, I-Worm.LovGate.h, Win32.Lovgate.I, Win32.Lovgate.K) (Win32 Worm): This is a variant of W32/Lovgate-A. W32/Lovgate-J is a worm, a virus and backdoor Trojan. The worm spreads across the local network by copying itself into folders with the various names. It also attempts to spread via e-mail by sending itself to e-mail addresses collected from *.HT* files. E-mails sent to these addresses can have the various subject lines, message texts and attachment names in any combination. The worm also attempts to reply to e-mails found in the user's inbox. W32/Lovgate-J copies itself into the Windows system folder as ravmond.exe, winhelp.exe, WinGate.exe, winrpc.exe, windriver.exe, iexplore.exe, and kernel66.dll and sets the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Remote Procedure Call Locator = "RUNDLL32.EXE reg678.dll ondll_reg"
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winhelp = "<Windows system folder>\winhelp.exe"
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WinGate initialize = "<Windows system folder>\WinGate.exe -remoteshell"
- HKLM\Software\CLASSES\txtfile\shell\open\command = "winrpc.exe %1"
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\COM+ Event System = DRWTSN16.EXE

On Windows NT the worm drops the files ily668.dll, task688.dll, reg678.dll, and win32vxd.dll into the Windows system folder. It drops DRWTSN16.EXE into the Windows folder. This component of W32/Lovgate-J is used to infect other EXE files on the local machine and on shares. The worm attempts to share the <Windows folder>\temp folder as "GAME" and drops several copies of itself into this folder with random filenames and the double extensions. W32/Lovgate-J attempts to terminate certain AV and other processes. W32/Lovgate-J is also a backdoor Trojan that provides a malicious user with unauthorized access to the user's computer and can send notification e-mail messages to the malicious user.

W32/Randon-I (Win32 Worm): This is a complex multipartite worm that spreads through IRC channels and shares, targeting computers with poorly configured usernames and passwords. The worm is usually distributed as a self-extracting archive which when executed installs the worm components to the Windows system folder. Various files are dropped. The worm may set the attributes of some extracted files hidden. Some of these files are used by the worm for hacking/spreading/running purposes. W32/Randon-I initiates

the main executable part, that is EXPL32.exe as a background process. This allows unauthorized access and control of the computer over IRC channels. The worm then sets the following registry keys to make sure this file will be executed at the next restart and upon running an IRC client software:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run = "<copy of EXPL32.exe>"
- HKLM\Software\CLASSES\ChatFile\DefaultIcon = "<copy of EXPL32.exe>"
- HKLM\Software\CLASSES\ChatFile\Shell\open\command = "<copy of EXPL32.exe>"
- HKLM\Software\CLASSES\irc\DefaultIcon = "<copy of EXPL32.exe>"
- HKLM\Software\CLASSES\irc\Shell\open\command = "<copy of EXPL32.exe>"

When installed, the background process connects to an IRC server and executes its scripts, allowing itself to function as a DoS attacker and IRC flooder. The worm also scans for open ports (445), searching for possible victims with poorly configured username and passwords, by running a batch file that attempts to locate and connect to a shared resource. To gain further access and control over the computer the worm uses a number of legitimate applications (some of the them listed below) that come packed with the worm components in the archive:

- Empavms.exe ("HideWindow" application)
- Libparse.exe ("PrcView" application)
- psexec.exe ("PsExec" application)

W32/Winur-D (Aliases: W32.HLLW.Purol, W32/Winur.worm.d, WORM_PUROL.A,

Worm.P2P.Purol.b) (Win32 Worm): This is a worm that exploits peer-to-peer networks such as BearShare, Morpheus, eDonkey2000, Gnucleus, KaZaA, KaZaA Lite, and LimeWire and also the file sharing capabilities of the ICQ messaging system. When executed, the worm copies itself to the Windows folder with the filenames lorupscr.scr, winstart32.exe, and hwinfoq.com and sets the following registry entries:

- HKCU\Control Panel\Desktop "ScreenSaveTimeOut"="300"
"SCRNSAVE.EXE"="C:\\windows\\lorupscr.scr"
- HKCU\Software\Microsoft\CurrentVersion\Run "Winstart"="C:\\windows\\winstart32.exe"
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
"Winstart"="C:\\windows\\winstart32.exe" HWINFOQ="C:\\windows\\HWINFOQ.com"

The worm attempts to delete all files from various antivirus folders. W32/Winur-D creates a C:\Windows\MyShares folder and copies the various files into it. W32/Winur-D also creates more than 500 copies of itself in the various folders using the filenames from a list and from the current folder. To be able to propagate through the networks the worm sets registry entries, e.g. setting C:\\windows\\MyShares folder as a My Shared Folder and enabling sharing. Every 10 seconds the worm attempts to initiate a DDoS attack via <ping www.whitepower.org -l 65500 -t>.

W32.Yaha.S@mm (Alias: I-Worm.Lentin.m): This is a variant of W32.Yaha@mm. This variant terminates some antivirus and firewall processes. The worm retrieves e-mail addresses from the Windows Address Book, the contact lists of MSN Messenger, .NET Messenger, Yahoo Pager, and ICQ. It also retrieves e-mail addresses from the files whose extensions contain the letters HT. W32.Yaha.S@mm uses its own SMTP engine to e-mail itself to the e-mail addresses it finds. The e-mail message has a randomly chosen subject line, message, and attachment. The attachment will have a .exe or .scr file extension. This threat is written in the Microsoft C++ language and is compressed with UPX.

WORM_LOVELORN.B (Aliases: W32/Lovelorn@MM, I-Worm.Lovelorn.b, Win32.Lovelorn.B worm) (Internet Worm): This variant of WORM_LOVELORN.A similarly spreads via e-mail using its built-in SMTP (Simple Mail Transfer Protocol) engine. It sends an e-mail using various subjects, message bodies, attachments and senders. This mailer gets its target recipients from files with names that contain any of these strings: .EML, ITEM, BOX, .DBX, or .HTM. It also carries file infection routines but due to bugs in its codes, this intended routine is not always triggered. This mass-mailer also tries to copy itself to floppy disks and steals the user's passwords.

WORM_PALYH.A (Aliases: W32.HLLW.Mankx@mm, W32/Palyh@MM, W32/Palyh-A, I-Worm.Palyh, Win32.Palyh.A, W32.Sobig.B@mm) (Internet Worm): This worm has been reported in the wild and is spreading rapidly. It propagates by using its own SMTP engine to mass-mail copies of itself to other users. It sends e-mail with the following details:

- From: support@microsoft.com
- Subject: (any of the following) Approved (Ref: 38446-263), Cool screensaver \

This worm runs on Windows 95, 98, ME, NT, 2000, and XP.

Worm/Poopoo (Alias: Worm.P2P.Poopoo) (P2P Worm): This is a P2P Internet worm that spreads through the use of many popular file-sharing programs, as well as, through the use of the mIRC network. If executed, the worm will create the following files:

- C:\Mirc\script.ini
- C:\Mirc32\script.ini
- C:\Program Files\Mirc\script.ini
- C:\Program Files\Mirc32\script.ini
- C:\Poopoo.dat

Trojans

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

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.AntiLam.20.K	K	Current Issue
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	Current Issue
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	Current Issue
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	Current Issue
Backdoor.CNK.A	A	Current Issue

Trojan	Version	CyberNotes Issue #
Backdoor.CNK.A.Cli	Cli	Current Issue
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	Current Issue
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	Current Issue
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Fatroj	N/A	Current Issue
Backdoor.Fatroj.Cli	Cli	Current Issue
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	Current Issue
Backdoor.Fxdoor.Cli	Cli	Current Issue
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Lampsy	N/A	Current Issue
Backdoor.IRC.Ratsou	N/A	Current Issue
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.LeGuardien.B	B	Current Issue
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	Current Issue
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Snami	N/A	Current Issue
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	Current Issue
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07

Trojan	Version	CyberNotes Issue #
Backdoor.Udps.10	10	CyberNotes-2003-03
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	Current Issue
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Downloader.BO.B	B	Current Issue
Downloader.BO.B.dr	B.dr	Current Issue
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Seeker-C	C	CyberNotes-2003-04
JS_WEBLOG.A	A	CyberNotes-2003-05
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.ALlight	N/A	CyberNotes-2003-01
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	Current Issue
PWSteal.Lemir.105	105	Current Issue
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	Current Issue
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	Current Issue
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Watsn	N/A	Current Issue
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	Current Issue
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07

Trojan	Version	CyberNotes Issue #
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	N/A	CyberNotes-2003-02
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Peido-B	B	Current Issue
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	Current Issue
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	Current Issue
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS.Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09

Trojan	Version	CyberNotes Issue #
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systemtry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

Backdoor.AntiLam.20.K: This is a Backdoor Trojan Horse that gives a malicious user access to your computer. It is a minor variant of Backdoor.AntiLam.20. It makes some additional modifications to system files. When Backdoor.AntiLam.20.K is executed, it copies itself as %System%\internat.exe and attempts to delete the original Trojan file and creates the file, %System%\Scan.dll. If the operating system is Windows 95/98/ME, it makes the following modifications so that it runs when you start Windows: Modifies the shell= line of the [boot] section of the System.ini file to:

- shell=Explorer.exe C:\WINDOWS\SYSTEM\internat.exe

and adds the line, "run=C:\WINDOWS\SYSTEM\internat.exe," to the [windows] section of the Win.ini file. Next it adds the value, "SVCHOST"="%System%\internat.exe," to the following keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It also creates the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\KeyConfig

which contains the configuration information of the Trojan and adds the value, "Start"="ok," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\DirectX

It sets itself up as a server and listens for incoming connections on ports 29999 and 30303.

Backdoor.Beasty.Cli: This is the client component of the Backdoor.Beasty family of Trojan Horse programs. It allows a malicious user to remotely access a computer running a variant of Backdoor.Beasty.

Backdoor.CamKing (Alias: Trojan.Win32.Camking): Backdoor.CamKing This Trojan allows the author of this Trojan Horse to activate your computer's Web cam. Backdoor.CamKing uses sockets to connect to a compromised machine and activates the Web cam on the server to allow its author to spy on you. The author of Backdoor.CamKing can configure the ports. When Backdoor.CamKing is run, the server portion of the Trojan copies itself to %Windir%\OSLoader.exe and it adds the value, "OSLoader"="OSLoader.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows.

Backdoor.Cmjspy: This is a Backdoor Trojan Horse that logs keystrokes to compromise private information. When Backdoor.Cmjspy is executed, it copies itself to several files on the system, including:

- %System%\Fgdfd.exe
- %System%\Fgdfd.exe

Next it searches the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

for references to the files with the .exe extension. For each such entry, the Trojan copies itself as a the same filename, but with a single-space prior to the .exe. Then, Backdoor.Cmjspy changes the registry entry to call it rather than the intended file. This causes the Trojan to run when you start Windows. On startup, the malicious Scandisk.exe program will start Fgdfd.exe, plus the real Scandisk.exe program, so that the system still appears to behave normally and creates the following (non-viral) files in %System%:

- Tdllcope.vxd
- Systemdllx.vxd

- Cfgxix.xi (This file is subsequently deleted.)
- Hlicense.vxd (This file is used to store keylogging data.)
- Ppx.txt
- Ppkey.txt

Backdoor.CNK.A: This is a Backdoor Trojan Horse that gives the author of the Trojan access to your computer. When Backdoor.CNK.A is executed, it listens for a connection on port 2000. Once a connection is established, the malicious user can execute various commands. The Trojan does not modify the registry or drop any files. It does not have any built-in provisions to automatically execute on startup.

Backdoor.CNK.A.Cli: This is the client portion of the Backdoor.CNK.A Trojan Horse. Using the client, a malicious user can gain access to a computer running the corresponding Trojan Horse server, Backdoor.CNK.A. It establishes a connection on port 2000.

Backdoor.Death.Cli: This is the client portion of the Backdoor.Death Trojan Horse. Using the client, a malicious user can gain access to a computer running the Backdoor.Death server.

Backdoor.Delf.Cli: This is the client portion of the Backdoor.Delf family of Trojan Horses. Using the client, a malicious user can gain access to a computer running one of the Backdoor.Delf variants of Trojan Horse servers.

Backdoor.Fatroj: This is a Backdoor Trojan Horse that gives a malicious user access to your computer. When Backdoor.Fatroj is executed, it listens for an incoming connection on port 1011 or 10011. (This is the default setting, though the malicious user may choose a different port.) While the Trojan runs, a small image may appear in the top left corner of the Windows desktop, where it may partially cover any icon in that particular location. This Trojan does not modify the registry or drop any files by itself. It does not have any built-in provisions to automatically execute on startup; however, the malicious user can make such changes to your system once it has been compromised.

Backdoor.Fatroj.Cli: This is the client component of the Backdoor.Fatroj Trojan Horse. Using the client, a malicious user can gain unauthorized access to a computer running the corresponding Trojan Horse server, Backdoor.Fatroj. It contains a kit to create new Trojan Horse programs. The client opens connections on port 1011 or 10011, by default.

Backdoor.Fxdooor: This is a Backdoor Trojan Horse that gives a malicious user remote access to your computer. When Backdoor.Fxdooor is executed, it copies itself to the following files, and then deletes the original file:

- %Windir%\Sk.exe
- %System%\Plog.exe
- %System%\Swon4.exe

Next it adds the value, "Snow"="%Sysdir%\swon4.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. The line, "run=%Windir%\sk.exe," is added to the Win.ini file so that the Trojan runs when you start the Windows 95/98/ME systems. A network connection is opened on port 5328, by default and the Trojan listens for an incoming connection. Once a connection is established, a malicious user will be able to view and edit files, capture screenshots, and compromise the privacy and integrity of the infected system.

Backdoor.Fxdooor.Cli: This is the client portion of the Backdoor.Fxdooor Trojan Horse. Using the client, a malicious user can gain access to a computer running the corresponding Trojan Horse server, Backdoor.Fxdooor.

Backdoor.IRC.Lampsy: This is a Backdoor Trojan Horse that uses mIRC to communicate with a remote malicious user. It allows the Trojan's creator to fully control a compromised system. Backdoor.IRC.Lampsy typically arrives as a large executable file. It may be downloaded from predefined Web sites by Downloader.BO or Downloader.BO.B. When Backdoor.IRC.Lampsy runs, it creates the folder, C:\Winnt\User, and inserts the following files in it:

- B.eXe
- CL.eXe
- Drx2.INF
- Pr.eXe
- S3.eXe

It adds the value, "eXe"="c:\Winnt\User\By.eXe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that this patched mIRC client runs each time you start Windows. The Trojan connects to a predefined IRC server and logs into an IRC channel, through which the malicious user can control the Trojan.

Backdoor.IRC.Ratsou: This is a Backdoor Trojan that gives a malicious user full control of your computer. Backdoor.IRC.Ratsou may be downloaded by Trojan.Downloader.Aphe from the Web site, <http://amateur.freegayspace.com>. When Trojan.Downloader.Aphe runs, it may download a file as C:\Roof.exe from a specific Web site. Then, the Trojan executes C:\Roof.exe. C:\Roof.exe downloads a third file as C:\Newconf.exe from the same Web site and next the Trojan executes C:\Newconf.exe.

Backdoor.LeGuardien.B: This is a Backdoor Trojan Horse that gives a malicious user access to your computer. Because of the many dependencies of Backdoor.LeGuardien, it may not run as intended or it may display error messages on startup. When Backdoor.LeGuardien correctly executes, it displays a window with the text "Le Clavier !" in the title bar. This only happens the first time when the Trojan Horse is being installed. The Trojan installs itself as the file, %Windir%\Wintray.exe and adds the value, "WinTray"="%Windir%\wintray.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

It sets itself as a server, listening on port 1,001, plus one other port. A malicious user who connects to the server will now have full control of the computer.

Backdoor.Peers: This is a Backdoor Trojan Horse that gives a malicious user remote access to your computer. When executed, it adds the value, "SysCtl"="sysctl.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

so that the Trojan runs when you start Windows, if the Trojan is installed in the Windows folder. It adds the line, "run=%Windir%\sysctl.exe," to the [windows] section of the Win.ini file, so that the Trojan runs when you start Windows 95/98/ME. The Trojan starts a server, listening for incoming connections on port 8961. The Trojan does not copy itself or drop any other files.

Backdoor.Snami (Alias: Backdoor.Tsunami.b): This is a Backdoor Trojan Horse that attempts to connect to an IRC server and obtain instructions to execute on an affected system.

Backdoor.Softshell (Alias: Backdoor.NetMagik): This is a Backdoor Trojan Horse that gives a malicious user remote access to your computer. When Backdoor.Softshell is executed, it listens for incoming connections on ports 6711 and 6811. Once a connection is established, the malicious user has control of the computer and can transfer files or change system settings. The Trojan does not drop any files by itself and does not have provisions to automatically execute on startup.

Backdoor.Zdemon.126 (Aliases: Backdoor.Zdemon.125, BackDoor-ARP): This Trojan gives its author remote access to your computer. Although the listening ports are configurable, by default, the Trojan listens on ports 10001 and 10002. When Backdoor.Zdemon.126 is executed, it moves itself to the %System% folder as Z100.exe and appends Z100.exe to the shell= line of the System.ini file, so that the Trojan runs when you start Windows 95/98/ME computers. It adds the value, "Micro"="%system%\Z100.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. A port is opened that allows the Trojan's creator to remotely control an infected computer.

Downloader.BO.B: This is a Trojan Horse that downloads a Backdoor Trojan from predefined Web sites. This threat is compressed with UPX. When Downloader.BO.B runs, it creates the subkey, “.inr,” under the registry key:

- HKEY_LOCAL_MACHINE\Software\CLASSES

and creates the subkey, “hfEpMmUA6ggn4ulq,” under the .inr key and adds the following value to this subkey:

- "Time"="<the time that the Trojan was executed>"

Next the Trojan attempts to download the file l.exe from one of these predefined Web sites:

- www.t-shirts-shop.net
- 63.246.131.33

If the Trojan is successful in downloading the file, it locally saves the file as Output.exe, and then runs this downloaded file. Then, it adds the value, “(Default)”=“Done,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\CLASSES\.inr\hfEpMmUA6ggn4ulq

If the download fails, the Trojan adds the value, “.inr\hfEpMmUA6ggn4ulq”=“<the Trojan file name>,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows.

Downloader.BO.B.dr (Alias: Troj/Peido-B): This is a .html file that drops Downloader.BO.B onto the infected system. The existence of the file error.hta is an indication of a possible infection. This Trojan arrives disguised as an administrative e-mail, which may have the following characteristics:

- From: MAILER-DAEMON
- Subject: Warning: could not send message!
- Attachment: Error.hta

The e-mail is generated and distributed manually by a malicious user and is not a function of the Trojan Horse. If you open the attachment, it displays a fake message. Then, the Trojan creates a file on your computer as C:\windows\Sys_con.exe and then executes it.

PWS-Yipper (Alias: Trojan.Spy.Yitai): This Trojan proceeds to retrieve address entries from Outlook Address Book and sends it out in the e-mail format below:

- To: keren@netsite.com.br
- Subject: NewWorld

This Trojan also opens up a list of ports on the infected machine. The port range is between 1042-1055. This Trojan searches for system passwords and e-mail addresses on the local machine. Once this data is found it sends it to either of the following e-mail addresses:

- yitai342@012.net.il
- yipai342@netvison.net.il

The subject of the message it sends out may be either 'NewWorld' or 'Hi' The message body contains encrypted data which seems to be e-mail addresses stolen by the Trojan from the Outlook address book as well as system passwords. This Trojan does not copy itself to the local system and no registry entries were created/modified. The following filenames may be used by this Trojan:

- yitai.exe
- FindMyMatch.exe
- NikeStock.exe
- TeenViewer.exe

PWS-Watsn: This is a password stealing Trojan. The Trojan is likely to arrive in a self-extracting archive. When the dropper file is run, the following Trojan files are created in the Windows system directory:

- drwatson.exe
- rundll16.exe
- rundll32.exe

The following registry key is created so that the Trojan can run at Windows startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"DRWATSON.EXE" = c:\windows\system\DRWATSON.EXE

The Trojan dll can record keystrokes and save the information into an encrypted file. The file is sent via SMTP mail. The e-mail has the following characteristics:

- From:sservicos@yahoo.com.br
- To:ideal@netrouter.com.br
- Subject: IDEAL SISTEMA DE ENSINO ESCOLAR
- Attachment: 7350~.dat

PWSteal.Kipper: This is a password-stealing Trojan Horse that sends information about the following programs, as well as others, to the creator of the Trojan:

- Half-Life
- Tiberian Sun
- Medal of Honor Allied Assault
- Battlefield 1942

PWSteal.Lemir.105 (Alias: Trojan.PSW.Legendmir.105): This is a password-stealing Trojan Horse that attempts to steal the password for the "Legend of Mir 2" online game and send it to the creator of the Trojan. The password is e-mailed with a subject line, "www."

PWSteal.Rimd.B: This is a password-stealing Trojan horse that attempts to steal information from a Chinese online game. This Trojan horse then sends the information to the author of the Trojan. When PWSteal.Rimd.B is executed, it copies itself as %Windir%\Kernelbc.exe and creates the file, "System%\grilf.dll." Next it modifies the (Default) value of the registry key:

- HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command

to, "%windir%\kernelbc.exe "%1" %." This causes the Trojan to be executed each time that an executable file is run. The Trojan executes the file Grilf.dll, which is a component of the Trojan. This component hooks the mouse and keyboard so that a function in Grilf.dll will be called when the mouse or keyboard is used. The function called in Grilf.dll attempts to find a window that belongs to a Chinese online game. If found, it will save the account information from this window within the file %Windir%\kernel.ini. The Trojan Horse will then e-mail kernel.ini to the author of the Trojan.

PWSteal.Snatch (Alias: Trojan.PSW.AIM.Snitch): This is a Trojan horse program which mimics the AOL Instant Messenger client for the purpose of stealing passwords.

Troj/Peido-B (Aliases: VBS.Inor.B, TrojanDropper.VBS.Inor): This Trojan has been reported in the wild. It drops Troj/DLoader-BO and appears as an administrative e-mail containing the text " THIS IS A WARNING MESSAGE ONLY YOU DO NOT NEED TO RESEND YOUR MESSAGE." The attachment is called error.hta. The file sys_con.exe is placed in the Windows Folder and executed.

Trojan.Kaht (Alias: TROJ_Kaht.A): This is a Hacktool used by its creator to scan for and exploit the vulnerability of the Microsoft WebDAV server, running IIS 5.0. An individual who successfully exploits this vulnerability may completely control an affected Web server. Many applications use the vulnerable Win32 API component, ntdll.dll, so other attack vectors may exist. It is strongly recommended that all the users of Microsoft 2000 and NT audit their computers for the vulnerabilities, which are referred to in the Microsoft Security Bulletin MS03-007. The IIS WebDAV uses a core Windows system component, ntdll.dll, containing an unchecked buffer when processing the incoming WebDAV requests. Trojan.Kaht scans for the vulnerable Microsoft WebDAV (IIS 5.0) server, by sending a specially formatted WebDAV HTTP request to the server. If the server is vulnerable, the Trojan creates a script file, kaht.html, on the compromised system. Then, the Trojan adds a user, "KaHT," to the administrator group and spawns a shell. This action gives the Trojan's creator complete control of the system.

Trojan.Lear: This is a Trojan horse that is written in the Microsoft Visual Basic (VB) programming language. It requires VB runtime libraries to execute. This threat is compressed with ASPack. When Trojan.Lear runs, it copies itself as:

- %System%\Internet.exe
- %System%\Widows.exe

and adds the value, "interneter"="%system%\interneter.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

The Trojan also adds the value, "load"="%system%\widows.exe," to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

and adds the value, "Start Page"="http://www.dj3344.com," to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main