# National Infrastructure Protection Center
# CyberNotes

*Issue #2002-02* *January 28, 2002*

**CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.**

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

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, D.C., 20535.

## *Bugs, Holes & Patches*

The following table provides a summary of software vulnerabilities identified between January 10 and January 24, 2002. 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 |
|---|---|---|---|---|---|---|---|
| ACD Incorporated[1] | Multiple | CwpAPI 1.1 | A vulnerability exists in the 'GetRelativePath' function because paths are not checked properly, which could let a malicious user obtain sensitive information. | Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=39378&release_id=69915 | CwpAPI Path Validation | Medium | Bug discussed in newsgroups and websites. |

[1] ACD Incorporated Security Advisory, January 22, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Activestate[2] | Windows | Active Python 2.1, Activestate win32all | A vulnerability exists due to the default policy associated with the RExec class, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | ActivePython Weak Default Security Policy | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Alcatel[3] | Multiple | Speed Touch Home ADSL | A remote Denial of Service vulnerability exists when a malicious user scans the modem using NMap. | No workaround or patch available at time of publishing. | Speed Touch Home ADSL Denial of Service | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Ambrosia Software[4] | Unix | Maelstrom GPL 3.0.1 | A vulnerability exists due to the insecure way the file '/tmp/f' is created, which could let a malicious user overwrite arbitrary files. | No workaround or patch available at time of publishing. | Maelstrom Insecure Symbolic Link | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Apple[5] | MacOS X 10.0-10.0.4, 10.1-10.1.2 | Palm Desktop 4.0b77, 4.0b76 | A vulnerability exists because when folders and files are backed up by the synchronizing program they are created with world-readable permissions (even if the settings are manually changed), which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Palm Desktop For MacOS X Insecure Backup Permissions | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Askey Computer Corpora-tion[6] | Multiple | ADSL Router RTA-020 | A Denial of Service vulnerability exists when a router is configured with an IP address and portscanned by a scanning tool. | No workaround or patch available at time of publishing. | ADSL Router Denial of Service | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |

[2] Bugtraq, January 15, 2002.
[3] Securiteam, January 17, 2002.
[4] Bugtraq, January 20, 2002.
[5] Securiteam, January 16, 2002.
[6] Bugtraq, January 15, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Avirt[7] | Windows 95/98/ME/ NT 4.0/2000, XP | Gateway 4.2, Suite 4.2, SOHO 4.2 | Several vulnerabilities exist: a buffer overflow vulnerability exists in the HTTP and Telnet proxies, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the implementation of the Telnet proxy, which could let a malicious user obtain sensitive information or SYSTEM privileges. | No workaround or patch available at time of publishing. | Gateway Suite HTTP and Telnet Remote Buffer Overflow and Telnet Proxy Remote Access | **High** | Bug discussed in newsgroups and websites. |
| BAL Crew[8] | Windows, Unix | COWS CGI Online Worldweb Shopping 1.1 | Multiple vulnerabilities exist: several Cross-Site Scripting vulnerabilities exist, which could let a malicious user execute arbitrary code; a vulnerability exists because sensitive information is not encrypted, which could let a malicious user obtain sensitive information; and a vulnerability exists because files are created with world-readable permissions, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | COWS CGI Online Worldweb Shopping Multiple Vulnerabilities | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Black Moon[9] | Windows 2000, XP | BlackMoon FTP Server 1.0-1.5 | A buffer overflow vulnerability exists when a long sequence of characters is supplied to the USER, PASS, or CWD commands, which could let a malicious user execute arbitrary code. | Upgrade available at: **http://members.rogers.com/blackmoon2k/bmftp152.zip** | BlackMoon Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Caldera[10] | Unix | UnixWare 7.1.1 | A vulnerability exists in the 'scoadminreg.cgi' program because user input is not properly validated, which could let a malicious user execute arbitrary code with administrative privileges. | No workaround or patch available at time of publishing. | UnixWare SCOAdmin Reg.CGI Validation | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |

[7] Strumpf Noir Society Advisories, January 17, 2002.
[8] Vuln-Dev, January 21, 2002.
[9] Strumpf Noir Society Advisories, January 15, 2002.
[10] Bugtraq, January 20, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| CDRDAO[1] [1] | Unix | CDRDAO 1.1.4, 1.1.5 | A vulnerability exists in the '.cdrdao' file, which could let a malicious user execute arbitrary commands as root. | No workaround or patch available at time of publishing. | CDRDAO Configuration File Symbolic Link | **High** | Bug discussed in newsgroups and websites. Exploit scripts have been published. |
| Chinput[12] | Unix | Chinput 3.0 | A buffer overflow vulnerability exists in the 'HOME' environment variable, which could let a malicious user execute arbitrary code as root. | No workaround or patch available at time of publishing. | Chinput Environment Variable Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| chuid[13] | Multiple | chuid 1.0-1.2 | A vulnerability exists because user-supplied input is not properly validated, which could let a remote malicious user change the ownership or group membership of restricted or privileged files. | Upgrade available at: **http://srparish.net/scripts/chuid-1.3.tar.gz** | CHUID File Input Validation | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Cisco Systems[14] | Unix | Billing and Management Server, PGW 2200, SC2200, Voice Services Provisioning Tool, VSC3000 | Vulnerabilities exist in the Media Gateway Controller (MGC) product, which could let a malicious user use the system for unauthorized purposes. | More information and patches available at: **http://www.cisco.com/warp/public/707/Solaris-for-MGC-pub.shtml** | Cisco Media Gateway Controller Vulnerability Exposure | **High** | Bug discussed in newsgroups and websites. Exploits have been published. |
| Citrix[15] | Multiple | Nfuse 1.6 | A vulnerability exists if a request for 'applist.asp' is submitted without authentication, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Nfuse 'applist.asp' Information Leak | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| ClanLib[16] | Unix | ClanLib 5.0 | A vulnerability exists in the way extremely long environment variables are handled, which could let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | ClanLib Environment Variable | **High** | Bug discussed in newsgroups and websites. |

[11] Securiteam, January 17, 2002.
[12] SecurityFocus, January 16, 2002.
[13] Securiteam, January 23, 2002.
[14] Cisco Security Advisory, January 16, 2002.
[15] Bugtraq, January 22, 2002.
[16] Bugtraq, January 14, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Conectiva[17] | Unix | Linux 5.0, 5.1, 6.0 | A vulnerability exists due to a flaw in the implementation of MySQL, which could let a malicious user obtain sensitive information. | Upgrade available at: **ftp://atualizacoes.conectiva.com.br/** | Linux MySQL Implementa-tion | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Cyberstop[18] | Windows 95/98/NT 4.0/2000 | Cyberstop Web Server for Windows 0.1 | Two Denial of Service vulnerabilities exist: a vulnerability exists if a request is submitted containing an unusual number of arbitrary characters; and a vulnerability exists when a URL request for a MS-DOS device name is submitted. | No workaround or patch available at time of publishing. | Cyberstop Web Server Denial of Service and MS-DOS Device Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit script has been published for the Long Request vulnerability. There is no exploit code required for the MS-DOS vulnerability. |
| Daan Systems[19] | Windows 95/98/ME/ NT 4.0/2000, XP | News Reactor 1.0 | A vulnerability exists because the password is stored insecurely, which could let a malicious user obtain sensitive information and unauthorized access. | No workaround or patch available at time of publishing. | NewsReactor Insecure Password | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| dnrd[20] | Unix | dnrd 1.0-2.10 | A remote Denial of Service vulnerability exists due to insufficient bounds checking to the DNS request and reply functions. | No workaround or patch available at time of publishing. | DNRD Bounds Checking Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

[17] Conectiva Linux Security Announcement, CLA-2002:455, January 18, 2002.
[18] Securiteam, January 22, 2002.
[19] Securiteam, January 22, 2002.
[20] Bugtraq, January 20, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| efax[21] | Unix | efax 0.8a, 0.9a, 0.9 | Two vulnerabilities exist: a buffer overflow vulnerability exists due to improper bounds checking on command line options, which could let a malicious user execute arbitrary code; and a vulnerability exists in the '-d' command line switch, which could let a malicious obtain sensitive information. *Note: If efax is installed setuid root, a malicious user can obtain root privileges.* | No workaround or patch available at time of publishing. | EFax UUCP Buffer Overflow and '-d' Command Line File Reading | **High** | Bug discussed in newsgroups and websites. There is no exploit code required for the Arbitrary File Reading vulnerability. |
| Enlighten-ment[22] | Unix | Imlib2 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4 | A buffer overflow vulnerability exists when the '$HOME' environment variable is filled with 4128 bytes and Eterm is executed, which could let a malicious user execute arbitrary code. | Update available at: **http://prdownloads.sourceforge.net/enlightenment/** | IMLib2 '$Home' Environment Variable Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| EServ[23] | Windows 95/98/NT 4.0 | EServ 2.92-2.97 | A vulnerability exists which could let a malicious user bypass password restrictions and obtain privileged access to the administrative directory. | Update available at: **ftp://ftp.eserv.ru/pub/beta/2.98/Eserv3119.zip** | EServ Password Restriction | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Francisco Burzi[24] | Multiple | PHP-Nuke 1.0, 2.5, 3.0, 4.0, 4.3, 4.4, 4.4.1a, 5.0, 5.0.1, 5.1, 5.2a, 5.2, 5.3.1 | A vulnerability exists due to insufficient input validation in the 'index.php' script, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | PHP-Nuke Input Validation | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Francisco Burzi[25] | Multiple | PHP-Nuke 1.0, 2.5, 3.0, 4.0, 4.3, 4.4, 4.4.1a, 5.0, 5.0.1, 5.1, 5.2a, 5.2, 5.3.1, 5.4 | A vulnerability exists in the 'sql_layer.php' script debugging feature, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | PHPNuke Debug Information Disclosure | Medium | Bug discussed in newsgroups and websites. Exploits have been published. |

[21] Bugtraq, January 16, 2002.
[22] Securiteam, January 17, 2002.
[23] VulnWatch, January 10, 2002.
[24] Bugtraq, January 17, 2002.
[25] Bugtraq, January 18, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| FreeBSD[26] | Unix | FreeBSD 4.x Heimdal Port 0.4e, 5.x Heimdal Port 0.4e, FreeBSD 4.0-4.4; KTH Heimdal 0.4e | A vulnerability exists in the 'getlogin()' function, which could let a malicious user obtain root privileges. | Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ | Kerberos 'getlogin()' Function | High | Bug discussed in newsgroups and websites. There is no exploit code required. |
| FreeWnn[27] | Unix | FreeWnn 1.1 | A vulnerability exists because input to the jserver component is not sanitized, which could let a malicious user execute arbitrary code. | Upgrade available at: ftp://ftp.etl.go.jp/pub/FreeWnn/alpha/FreeWnn-1.1.1-a017.tar.gz | FreeWnn Jserver Input | High | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Funsoft[28] | Windows 95/98/ME | Dino's Webserver 1.0, 1.2 | A Directory Traversal vulnerability exists when specifying a relative path, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Dino's Webserver Directory Traversal | Medium | Bug discussed in newsgroups and websites. |
| Geeklog[29] | Unix | Geeklog 1.3 | A security vulnerability exists in the permanent cookie authentication, which could let a malicious user access an administrative account. | Information is available at: http://geeklog.sourceforge.net | Geeklog Permanent Cookie Authentication | High | Bug discussed in newsgroups and websites. There is no exploit code required. |
| GNU[30] | Unix | groff 1.10, 1.11a, 1.11, 1.14-1.17 | A vulnerability exists due to insufficient bounds checking in the pre-processor, which could let a remote malicious user execute arbitrary commands. | Upgrade available at: ftp://updates.redhat.com/ | Groff Buffer Overflow<br><br>CVE Name: CAN-2002-0003 | High | Bug discussed in newsgroups and websites. |
| GNU[31] | Unix | Chess 5.02 | A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a malicious user execute arbitrary code. | Upgrade available at: ftp://ftp.gnu.org/pub/gnu/chess/chess-5.03beta.tar.gz | Chess Command Buffer Overflow | High | Bug discussed in newsgroups and websites. |

[26] FreeBSD Security Advisory, FreeBSD-SA-02:07, January 18, 2002.
[27] Shadow Penguin Security #44, January 11, 2002.
[28] Securiteam, January 14, 2002.
[29] Securiteam, January 17, 2002.
[30] Red Hat Security Advisory, RHSA-2002:004-06, January 14, 2002.
[31] Bugtraq, January 22, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| GNU[32], [33] | Unix | Enscript 1.4-1.6.1 | A vulnerability exists because temporary files are created insecurely in the 'tmpnam()' and 'tempnam()' functions, which could let a malicious user obtain elevated privileges. | **RedHat:** ftp://updates.redhat.com/ **Debian:** http://security.debian.org/dists/stable/updates/main/ | Enscript Insecure Temporary File Function | Medium | Bug discussed in newsgroups and websites. |
| Hewlett Packard Systems[34] | Unix | HP-UX 10.20, 11.0, 11.11 | A vulnerability exists in the "Diagnostic-Code:" field, which could let a malicious user obtain sensitive information about the mail system configuration. | Updates available at: http://itrc.hp.com PHNE_25183, PHNE_24419, PHNE_25184 | HP "Diagnostic-Code" Leakage | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| jmcce[35] | Unix | jmcce 1.3.8 | A vulnerability exists in the '/tmp' directory because it is not checked for the previous existence of a file, which could let a malicious user execute arbitrary code. | Update available at: http://www.mandrakesecure.net/en/ftp.php | jmcce Symbolic Link | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Joe Testa[36] | Multiple | hellbent 0.1 | Two vulnerabilities exist: a vulnerability exists when requests containing '../' sequences of a relative path is received, which could let a malicious user obtain sensitive information; and a vulnerability exists in the 'hellbent.prefs' file when a GET request is submitted, which could also let a malicious user obtain sensitive information. | Upgrade available at: http://hogs.rit.edu/~joet/code/hellbent_v011.zip | hellbent Relative Path Information Disclosure and 'hellbent.prefs' GET Request | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| John Roy[37] | Windows 95/98/NT 4.0/2000 | Pi3Web for Windows 2.0 | A buffer overflow vulnerability exists due to the way CGI parameters handle unusually crafted requests, which could let a malicious user execute arbitrary code. | Patch available at: http://sourceforge.net/tracker/download.php?group_id=17753&atid=317753&file_id=16364&aid=505583 | Pi3Web For Windows Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |

[32] Red Hat Security Advisory, RHSA-2002:012-06, January 17, 2002.
[33] Debian Security Advisory, DSA-105-1, January 22, 2002.
[34] Hewlett-Packard Company Security Bulletin, HPSBUX0201-179, January 16, 2002.
[35] Mandrake Linux Security Update Advisory, MDKSA-2002:008, January 22, 2002.
[36] Bugtraq, January 18, 2002.
[37] NTBugtraq, January 14, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Legato[38] | Windows NT 4.0/2000, Unix | NetWorker 6.1 | Vulnerabilities exist because sensitive information is stored in plaintext, which could let a malicious user obtain sensitive information and possibly elevated privileges. | Upgrade available at: http://portal1.legato.com/products/networker/ | NetWorker Plaintext | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Martin Roesch[39] | Unix | Snort 1.8.3 | A Denial of Service vulnerability exists if a maliciously constructed ICMP ECHO packet is sent to the server. | Patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/snort-icmp.patch | Snort ICMP Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Matt Wright[40] | Unix | FormMail 1.0-1.9 | Multiple vulnerabilities exist when inputs to the CGI script are manipulated, which could let remote malicious users send arbitrary e-mail messages. | No workaround or patch available at time of publishing. | FormMail SCI Script Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| MDG Computer Services[41] | Windows 98/NT 4.0, MacOS X 10.0 | Web Server 4D/ eCommerce 3.5.3 | A Directory Traversal vulnerability exists if a specially crafted URL is submitted, which could let an unauthorized malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Web Server 4D/ eCommerce Directory Traversal | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| MDG Computer Services[42] | Windows 98/NT 4.0, MacOS X 10.0 | Web Server 4D/ eCommerce 3.5.3 | A Denial of Service vulnerability exists when a long HTTP request is sent to the server. | No workaround or patch available at time of publishing. | Web Server 4D/ eCommerce Denial of Service | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Microsoft[43] | Windows 95/98/ME/ NT 4.0/2000 | Internet Explorer 5.5, 5.5SP1&2 | A Denial of Service vulnerability exists if a HTML form is crafted containing numerous characters as a value. | No workaround or patch available at time of publishing. | Internet Explorer Form Denial of Service | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Microsoft[44] | Windows 95 | Windows 95, 95 SR2 | A buffer overflow vulnerability exists due to the way large file extensions are handled, which could let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Microsoft Backup Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |

[38] Securiteam, January 16, 2002.
[39] Securiteam, January 20, 2002.
[40] Bugtraq, January 23, 2002.
[41] Securiteam, January 17, 2002.
[42] Securiteam, January 20, 2002.
[43] Bugtraq, January 15, 2002.
[44] Strumpf Noir Society Advisories, January 12, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[45] | Windows XP | Windows XP Home, Windows XP Professional | A Denial of Service vulnerability exists because the XML code is not properly verified. | No workaround or patch available at time of publishing. | Windows XP XML Denial of Service | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Microsoft[46] | Windows NT 4.0 | Windows 4.0, NT 4.0SP1-SP6a, NT Enterprise Server 4.0, 4.0SP1-SP6a, NT Workstation 4.0, 4.0SP1-SP6a | A vulnerability exists under some configurations because a locked account may still allow the machine to be unlocked locally. This may result in successful break-ins going undetected. | No workaround or patch available at time of publishing. | Windows NT Locked Account | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Microsoft[47] | MacOS 7.0/8.0/9.0 | Internet Explorer Macintosh Edition 3.0-4.0.1, 4.5, 5.0 | A vulnerability exists which could let a malicious webmaster execute arbitrary files, if the victim is using Internet Explorer 5 and the webmaster knows the file path. | No workaround or patch available at time of publishing. | MacOS Internet Explorer File Path | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[48] | Windows 95/98/ME/ NT 4.0/2000 | Internet Explorer 5.01, 5.0, 5.5, 6.0 | A vulnerability exists because access to the 'clipboardData' is provided without prompting the user, which could let a malicious user obtain sensitive information. | Workaround (Securiteam): Disable the functionality. Under the tools menu of IE, select Internet Options > Security > (select zone) > Custom Level. Under scripting, disable "Allow paste operations via script." or set it to "prompt" if you wish to be notified when this sort of operation is being conducted. | Internet Explorer 'clipboardData' | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |

[45] SecurityFocus, January 23, 2002.
[46] Bugtraq, January 21, 2002.
[47] Bugtraq, January 22, 2002.
[48] Securiteam, January 16, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[49] | Windows 98/ME/NT 4.0/2000 | Internet Explorer 6.0, Windows XP Professional | A vulnerability is created when upgrading to Windows XP Pro from previous versions of Windows because IE files are overwritten during the operating system software installation process, effectively re-setting the browser software back to original release version and removing all installed patches, including Q313675 (See MS01-058). | No workaround or patch available at time of publishing. | Windows XP Pro Upgrade | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Microsoft[50] | Windows 98/ME/NT 4.0/2000 | Internet Explorer 6.0 | A vulnerability exists when objects with a CODEBASE value are embedded in new objects created using in the 'PoPup()' or 'window.Open()' windows, which could let a remote malicious user execute arbitrary programs. | No workaround or patch available at time of publishing. | Internet Explorer Arbitrary Execution | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Multiple Vendors[51] | Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0-10.1.2, Unix | Mozilla Browser 0.9.2.1-0.9.6 Netscape Communicator 4.0-4.08, 4.5BETA, 4.5-4.78, 6.0 Mac, 4.77 Mac, 6.1, 6.2 | A vulnerability exists which could let a malicious user steal cookie-based authentication credentials because of the way NULL characters in URLs are handled. | **Mozilla Browser:** http://www.mozilla.org/releases/ **Netscape Communicator:** http://home.netscape.com/download/index.html | Netscape/ Mozilla Null Character | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Multiple Vendors[52] | Windows 98/ME/NT 4.0/2000, XP | Microsoft IIS 4.0, 5.0; Symantec Norton Internet Security 2001 | A vulnerability exists due to the default file system permissions in Windows, which could let an unauthorized malicious user manipulate the contents of log files. | **Workaround:** Microsoft recommends that you make the following changes on the appropriate: 1.Remove the IUSR_ ComputerName account. 2. Modify the permissions for the Everyone group to have only the appropriate permission by clicking "Read" in the "Type of Access" box. | Multiple Vendor Default File Permissions | Medium | Bug discussed in newsgroups and websites. |

[49] Jeffrey Dronenburg Advisory, #01-2002, January 15, 2002.
[50] Bugtraq, January 13, 2002.
[51] Bugtraq, January 21, 2002.
[52] Nomad Mobile Research Centre Advisory, January 14, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Multiple Vendors[53] | Windows 95/98/ME/ NT 4.0/2000, XP | Deerfield D2Gfx 1.0.2; Working Resources Inc. BadBlue 1.5 | A Directory Traversal vulnerability exists when a specially formatted request is submitted as a parameter to the script that reads Microsoft Office documents, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Multiple Vendor Directory Traversal | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Multiple Vendors[54] | Windows 95/98/ME/ NT 4.0/2000, XP | Deerfield D2Gfx 1.0.2; Working Resources Inc. BadBlue Enterprise Edition 1.5 | A vulnerability exists if the upload feature is configured without password protection, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Multiple Vendor Upload Feature Password Protection | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Multiple Vendors[55] | Multiple | Palm OS 3.5h | A Denial of Service vulnerability exists when a large amount of 'connect()' requests are received by the PDA. | No workaround or patch available at time of publishing. | PalmOS Remote Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Multiple Vendors[56], [57] | Unix | FreeBSD 2.0-4.4; NetBSD 1.3-1.5.2; OpenBSD 2.0-3.0 | A race condition vulnerability exists in the implementation of the 'exec()' system call, which could let a malicious user obtain elevated privileges. | **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:08/exec.patch **NetBSD:** ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2002-001-ptrace-1.4.patch | BSD exec() Race Condition | Medium | Bug discussed in newsgroups and websites. |

[53] Strumpf Noir Society Summaries, January 21, 2002.
[54] Strumpf Noir Society Summaries, January 21, 2002.
[55] Bugtraq, January 10, 2002.
[56] NetBSD Security Advisory, 2002-001, January 16, 2002.
[57] FreeBSD Security Advisory, FreeBSD-SA-02:08, January 24, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Multiple Vendors[58] | Windows 95/98/ME/ NT 4.0/2000, MacOS 9.0, Unix | AccessData SecureClean v3 build-2.0; East-Tec Eraser 2000, 5.3; Jetico BCWipe 1.07, 2.08b, 2.0, 2.13, 2.16, 2.28, 2.28.3, 2.28.4, 2.28.7, 2.33, 2.35, 2.35.1; Network Associates PGP 6.0.2, 6.5.3, 6.5.8, 7.0, 7.0.3, 7.0.4, 7.1.1, PGP Freeware 7.0.3 | A vulnerability exists in multiple file-wiping utilities because the data contained in Alternate Data Streams may not be properly removed. One possible consequence of this issue is that a user will not be able to use the standard methods to remove potentially malicious data from their system. | No workaround or patch available at time of publishing. | Multiple Vendor File Wiping Utilities | Medium | Bug discussed in newsgroups and websites. There is no exploit code required.<br><br>Vulnerability has appeared in the press and other public media. |
| Multiple Vendors[59], [60], [61], [62] | Unix | AT 3.1.7, 3.1.8 | A vulnerability exists because input isn't properly handled when scheduling a task via the commandline execution, which could let a malicious user execute arbitrary code with administrative privileges. | **SuSE:** ftp://ftp.suse.com/pub/suse/ **Debian:** http://security.debian.org/dists/stable/updates/main/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/ | AT Command line Execution<br><br>CVE Name: CAN-2002-0004 | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Netgear[63] | Multiple | RP114 Cable/DSL Web Safe Router<br><br>Firmware 3.26 | A Denial of Service vulnerability exists if the router is configured to drop packets intended for ports 1024 and below. | No workaround or patch available at time of publishing. | RP114 Cable/DSL Web Safe Router Denial of Service | Low | Bug discussed in newsgroups and websites. This vulnerability can be exploited with a port scanning utility. |

[58] KSSA-003, January 20, 2002.
[59] SuSE Security Announcement, SuSE-SA:2002:003, January 16, 2002.
[60] Debian Security Advisory, DSA 102-2, January 18, 2002.
[61] Mandrake Linux Security Update Advisory, MDKSA-2002:007, January 18, 2002.
[62] Red Hat Security Advisory, RHSA-2002:015-13, January 22, 2002.
[63] Bugtraq, January 15, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Netopia[64] | MacOS | Timbuktu Pro for Macintosh 6.0.1 | A Denial of Service vulnerability exists if a large number of connections are created to the server. | No workaround or patch available at time of publishing. | Timbuktu Pro Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Nevrona Designs[65] | Windows NT | MiraMail 1.04 | A vulnerability exists due to the way variables (i.e., account usernames and passwords) are stored in plaintext, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | MiraMail Plain Text Storage | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Nullsoft[66] | Windows 95/98/ME/ NT 4.0/2000 | Shoutcast Server 1.8.3 Win32 | A remote Denial of Service vulnerability exists when a long backslash string request is made from the 'admin.cgi' script. | No workaround or patch available at time of publishing. | Shoutcast 'Admin.CGI' Denial of Service | Low | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| Olaf Titz[67], [68] | Unix | CIPE 1.0.1, 1.1, 1.2, 1.3, 1.4.5, 1.4.6, 1.5.2 | A Denial of Service vulnerability exists if a CIPE packet is received that is shorter than it should be. | **Debian:** http://security.debian.org/dists/stable/updates/main/ **RedHat:** ftp://updates.redhat.com/ | CIPE Denial of Service CVE Name: CAN-2002-0047 | Low | Bug discussed in newsgroups and websites. |
| OpenLDAP[69] | Unix | OpenLDAP 2.0-2.0.7 | Two vulnerabilities exist: a vulnerability exists which could let a malicious user delete object attributes; and a vulnerability exists because permissions are not checked in access control lists, which could let a malicious user remove object attributes. | Upgrade available at: ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/openldap-2.0.21.tgz **RedHat:** ftp://updates.redhat.com/ | OpenLDAP Object Attribute Deletion and Access Control Permissions | Medium | Bug discussed in newsgroups and websites. An LDAP client can be used to exploit this vulnerability. |
| Oracle Corporation[70] | Multiple | Oracle8i 8.0.1, 8.0.2, 8.0.4-8.0.6, 8.1.5-8.1.7.1, Oracle9i 9.0, 9.0.1 | A vulnerability exists in the demo account for the RDBMS server due to preset passwords, which could let a remote malicious user obtain unauthorized access to the database. | No workaround or patch available at time of publishing. | Oracle RDBMS Demo Account | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |

[64] Bugtraq, January 18, 2002.
[65] Securiteam, January 16, 2002.
[66] Bugtraq, January 22, 2002.
[67] Debian Security Advisory, DSA-104-1, January 14, 2002.
[68] Red Hat Security Advisory, RHSA-2002:007-16, January 22, 2002.
[69] Red Hat Security Advisory, RHSA-2002:014-07, January 22, 2002.
[70] SecurityFocus, January 17, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Oracle Corporation[71] | Multiple | Oracle8i 8.0.1, 8.0.2, 8.0.4-8.0.6, 8.1.5-8.1.7.1 | A remote Denial of Service vulnerability exists if either of the 'dbsnmp_start' or 'dbsnmp_stop' commands are sent remotely to the TNS listener service. | No workaround or patch available at time of publishing. | Oracle 8i Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Oracle Corporation[72] | Multiple | Oracle8i 8.0.2, 8.0.4-8.0.6, 8.1.5-8.1.7.1, Oracle9i 9.0, 9.0.1 | A vulnerability exists in the default settings of SQL*Plus, which could let a malicious user execute arbitrary shell commands. | No workaround or patch available at time of publishing. | Oracle SQL*Plus Default Settings | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Oracle Corporation[73] | Multiple | Oracle8i 8.0.2, 8.0.4-8.0.6, 8.1.5-8.1.7.1, Oracle9i 9.0, 9.0.1 | A vulnerability exists in the default configuration because auditing is disabled, which could let malicious activity go undetected. | No workaround or patch available at time of publishing. | Oracle Default Auditing Configuration | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| PaintBBS[74] | Multiple | PaintBBS 1.2 | A vulnerability exists because the configuration file and the 'cgi-bin' directory are world readable, which could let a remote malicious user obtain sensitive information including the administration password. | No workaround or patch available at time of publishing. | PaintBBS Configuration File and 'cgi-bin' Directory | **High** | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| PHP Group[75] | Unix | PHP 4.0.4- 4.0.6, 4.1- 4.1.1 | A vulnerability exists because Session IDs are not stored in a secure environment, which could let an unauthorized malicious user gain privileged access. | No workaround or patch available at time of publishing. | PHP4 Session IDs | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Pi-Soft[76] | Windows 95/98/ME/ NT 4.0/2000 | SpoonFTP 1.1.0.1, 1.00.13, 1.00.12, 1.0, 1.1 | A vulnerability exists which could let a malicious user use the 'PORT' command to connect to a remote host. | Upgrade available at: **http://www.pi-soft.com/spoonftp/sftp.exe** | SpoonFTP 'PORT' Command | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |

[71] SecurityFocus, January 18, 2002.
[72] SecurityFocus, January 17, 2002.
[73] SecurityFocus, January 18, 2002.
[74] Bugtraq, January 23, 2002.
[75] Securiteam, January 15, 2002.
[76] Bugtraq, January 20, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| plDaniels[77] | Unix | RipMime 1.2.0-1.2.6 | A buffer overflow vulnerability exists in the way filenames are handled, which could let a malicious user execute arbitrary code and obtain elevated privileges. | Upgrade available at: **http://pldaniels.org/ripmime/ripmime-1.2.7.tar.gz** | RipMime Filename Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| psyBNC[78] | Unix | psyBNC 2.3 | A vulnerability exists which could let a malicious user add plaintext messages into an encrypted conversation. | Upgrade available at: **http://www.psychoid.lam3rz.de/psyBNC2.3.tar.gz** | psyBNC Encrypted Conversation | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Sambar Technologies[79] | Windows 95/98/ME/ NT 4.0/2000 | Sambar Server 5.1 | A Denial of Service vulnerability exists when consecutive excessively long requests are sent to the 'cgitest.exe' sample script. This could possibly let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Sambar Server Denial of Service | Low/**High** **(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Sapporo Works[80] | Windows 2000 | Black JumboDog 2.6.4, 2.6.5 | A buffer overflow vulnerability when an excessively long "expires," "if-modified-since," or "Last_Modified," string is sent, which could let a malicious user execute arbitrary code. | Upgrade available at: **http://my.vector.co.jp/servlet/System.FileDownload/download/http/0/155232/pack/win95/net/network/bjd-patch-2.6.6.exe** | Black JumboDog Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| SGI[81] | Unix | IRIX 6.4, 6.5, 6.5.1, 6.5.2m, 6.5.2f, 6.5.2, 6.5.3m, 6.5.3f, 6.5.3, 6.5.4m/f-6.5.11m/f | A remote Denial of Service vulnerability exists due to the way the unified name service daemon (nsd) manages cache files. | Download the IRIX 6.5.12 or later Maintenance Release Stream available at: **http://support.sgi.com/colls/patches/tools/relstream/index.html** | IRIX nsd Denial of Service<br><br>CVE Name: CAN-2002-0038 | Low | Bug discussed in newsgroups and websites. |
| Siemens[82] | Multiple | 3568i WAP | A Denial of Service vulnerability exists if a maliciously formed SMS message contains certain unusual characters. | No workaround or patch available at time of publishing. | Siemens Mobile Phone Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |

[77] SecurityFocus, January 23, 2002.
[78] Bugtraq, January 22, 2002.
[79] VulnWatch, January 16, 2002.
[80] Shadow Penguin Security Advisory #42, January 10, 2002.
[81] SGI Security Advisory, 20020102-03-P, January 16, 2002.
[82] Xfocus, January 14, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Slashcode[83] | Unix | Slashcode 2.1-2.2.2 | A vulnerability exists which could let a malicious user obtain access to administrative accounts and take full control of the site. | Upgrade available at: **http://sourceforge.net/project/showfiles.php?group_id=4421** | Slashcode Administrative Account | **High** | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| Sniffit[84] | Unix | Sniffit 0.3.7beta | A buffer overflow vulnerability exists if Sniffit is configured to log e-mail messages, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Sniffit Mail Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Squirrel Mail[85] | Unix | SquirrelSpell 0.3.5 | A vulnerability exists in the SquirrelSpell plugin, which could let a malicious user execute arbitrary commands. | Patch available at: **http://www.dulug.duke.edu/~icon/misc/security_fix.sh.txt** | SquirrelSpell Plugin | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Squirrel Mail[86] | Unix | SquirrelMail 1.2.2 | Multiple vulnerabilities exist in the 'compose.php' script that could let a malicious user send malicious HTML messages that appear to come from a valid user or that would run arbitrary JavaScript. | Upgrade available at: **http://www.squirrelmail.org/download.php** | SquirrelMail 'compose.php' Script | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |

[83] SA-2002:00, January 10, 2002.
[84] Securiteam, January 22, 2002.
[85] Bugtraq, January 24, 2002.
[86] Bugtraq, January 24, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Todd Miller[87], [88], [89], [90], [91], [92], [93] | Unix | Sudo 1.6.3-1.6.3p7 | A vulnerability exists because sudo does not properly sanitize the environment with which it executes programs, which could let an unauthorized malicious user execute commands as root and potentially gain elevated privileges. | **Todd Miller:** http://www.sudo.ws/sudo/dist/sudo-1.6.4.tar.gz **SuSE:** ftp://ftp.suse.com/pub/suse/ **Engarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **Debian:** http://security.debian.org/dists/stable/updates/main/ **RedHat:** ftp://updates.redhat.com/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/security/sudo-1.6.4.1.tgz **Wirex:** http://download.immunix.org/ImmunixOS/7.0/updates/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ | Sudo Environment Variable | High | Bug discussed in newsgroups and websites. Exploit script has been published. |
| W3Perl[94] | Windows NT 4.0/2000, Unix | W3Perl 2.81-2.85 | A vulnerability exists because log file data is not sufficiently sanitized, which could let a malicious user execute arbitrary code. | Upgrade available at: http://www.w3perl.com/download/ | W3Perl Log File | High | Bug discussed in newsgroups and websites. This issue may be exploited using a utility such as Telnet to craft a raw HTTP header. |
| Working Resources Inc.[95] | Windows 95/98/ME/ NT 4.0/2000, XP | BadBlue 1.5 | A Denial of Service vulnerability exists if a request is made for a non-existent file. | No workaround or patch available at time of publishing. | BadBlue Denial of Service | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |

[87] SuSE Security Announcement, SuSE-SA:2002:002, January 14, 2002.
[88] EnGarde Secure Linux Security Advisory, ESA-20020114-001, January 14, 2002.
[89] Debian Security Advisory, DSA 101-1, January 14, 2002.
[90] RedHat Security Advisory, RHSA-2002:011-06, January 15, 2002.
[91] FreeBSD Security Advisory, FreeBSD-SA-02:06, January 16, 2002.
[92] Immunix OS Security Advisory, IMNX-2002-70-001-01, January 17, 2002.
[93] Trustix Secure Linux Security Advisory #2002-0021, January 18, 2002.
[94] Bugtraq, January 23, 2002.
[95] Strumpf Noir Society Summaries, January 21, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| YAMA-GUCHI [96] | Unix | Shingo beep2 1.0a, beep2 1.0, beep2 1.1, beep2 1.2 | A vulnerability exists in the command line input, which could let a malicious user obtain sensitive information. | Upgrade available at: http://www.kip.iis.toyama-u.ac.jp/~shingo/beep/package/src/beep2-1.2a.tar.gz | Shingo beep2 Command Line | Medium | Bug discussed in newsgroups and websites. |

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

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

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

**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 January 10 and January 24, 2002, 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, 22 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 |
|---|---|---|
| January 24, 2002 | Sparc.zip | A document that describes buffer overrun vulnerabilities on Sun Microsystems SPARC machines. |
| January 24, 2002 | Win32format.doc | A document on Windows 2000 format string vulnerabilities that includes a detailed discussion of how format string vulnerabilities exist in fprintf(), vprintf() and sprintf() calls, and how they are created, discovered, and exploited. |
| **January 22, 2002** | **Cyber_dos.pl** | **Script which exploits the Cyberstop Web Server Long Request Denial of Service vulnerability.** |
| **January 22, 2002** | **Sniffit-ex.c** | **Script which exploits the Sniffit Mail Logging Buffer Overflow vulnerability.** |

[96] Shadow Penguin Security #45, January 11, 2002.

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| January 21, 2002 | Debian-uucp.tar.gz | Script which exploits the Debian uucp vulnerability. |
| **January 20, 2002** | **Scoadminreg-ex.sh** | **Exploit for the Caldera UnixWare WebTop SCOAdminReg.CGI Arbitrary Command Execution vulnerability.** |
| January 18, 2002 | Attn.tar.gz | Script which exploits the AT Maliciously Formatted Time Heap Overflow vulnerability. |
| **January 18, 2002** | **Dbsnmp.c** | **Script which exploits the Oracle 8i dbsnmp Command Remote Denial of Service vulnerability.** |
| January 18, 2002 | Steghide-0.4.3.tar.gz | A steganography program which hides bits of a data file in some of the least significant bits of another file in such a way that the existence of the data file is not visible and cannot be proven. |
| **January 17, 2002** | **Cdrdao_show_file.sh** | **Exploit for the CDRDAO Home Directory Configuration File Symbolic Link vulnerability.** |
| **January 17, 2002** | **Cdrdaohack.sh** | **Exploit for the CDRDAO Home Directory Configuration File Symbolic Link vulnerability.** |
| January 17, 2002 | Execve.c | Script which exploits the IMLib2 Home Environment Variable Buffer Overflow vulnerability. |
| **January 16, 2002** | **Chinput_exp.c** | **Script which exploits the Chinput Environment Variable Buffer Overflow vulnerability.** |
| January 16, 2002 | Exploit.html | Exploit for the Microsoft Internet Explorer Clipboard Reading vulnerability. |
| January 16, 2002 | Sudo-xpl.sh | Script which exploits the Sudo Unclean Environment Variable Root Program Execution vulnerability. |
| **January 14, 2002** | **Smsdos.zip** | **Exploit for the Siemens Mobile Phone SMS Denial of Service vulnerability.** |
| January 14, 2002 | Sudo-postfix-ex.sh | Script which exploits the Sudo Unclean Environment Variable Root Program Execution vulnerability. |
| January 12, 2002 | Lkh-1.1.tgz | LKH is a very powerful and documented kernel function hooking library running on Linux 2.4/x86. The code has been explained and the API described in Phrack #58. |
| January 11, 2002 | Nikto-current.tar.gz | Nikto is a PERL, open source web server scanner that supports SSL and is based on LibWhisker. |
| January 11, 2002 | Raccess-0.6.tar.gz | "Remote Access Session" is a security tool to analyze the integrity of systems. The program tries to gain access to a system using the most advanced techniques of remote intrusion. |
| January 11, 2002 | Wnn_mkdir.c | Script which exploits the FreeWnn jserver JS_MKDIR Metacharacter Command Execution vulnerability. |
| January 10, 2002 | Bjd_264.c | Script which exploits the SapporoWorks Black JumboDog HTTP Proxy Buffer Overflow vulnerability. |

## Trends

- **The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in CA-2001-31 and discussed in VU#172583. For more information see CERT® Advisory CA-2002-01, located at: http://www.cert.org/advisories/CA-2002-01.html.**

- **NIPC has updated their advisory, NIPC Advisory 01-030, regarding what Microsoft refers to as a critical vulnerability in the universal plug and play (UPnP) service in Windows. For more information see, NIPC ADVISORY 01-030.3, located at: www.nipc.gov/warnings/advisories/2001/01-030-2.htm.**

# *Viruses*

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *Note: At times, viruses may contain names or content that may be considered offensive.*

| Ranking | Common Name | Type of Code | Trends | Date |
|---|---|---|---|---|
| 1 | W32/BadTrans | Worm | Stable | April 2001 |
| 2 | W32/SirCam | Worm | Stable | July 2001 |
| 3 | W32/Nimda | File, Worm | Stable | September 2001 |
| 4 | W32/Hybris | File, Worm | Stable | November 2000 |
| 5 | W32/Goner | Worm | Stable | December 2001 |
| 6 | W32/Magistr-(A &B) | File, Worm | Stable | March 2001 |
| 7 | W32/Funlove | File | Stable | November 1999 |
| 8 | W32/Gokar | File, Worm | New to table | December 2001 |
| 9 | W32/Apology (MTX) | File Infector, Trojan | Stable | September 2000 |
| 10 | VBS/SST (Anna K) | Script, Worm | Return to Table | February 2001 |

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **198** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **449** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

**ELF_RST.A (Aliases: RST.b, RST.A) (Elf Executable Virus):** This backdoor program runs on Linux/UNIX platforms. An infected system sends a signal through the network and listens for traffic on certain ports. It compromises system security, but has no destructive payload.

**HLLP.Saywat.7499 (DOS Virus):** This is a memory-resident DOS virus. It is written in the high-level language C++ and is packed using PKLITE. When the virus is executed, it stays in memory and infects .exe and .com files that are in the same folder as the virus. This virus prepends itself to files that it infects.

**VBS.Funcess (Visual Basic Script Worm):** This is a Visual Basic Script (VBS) worm that attempts to send itself by mIRC and Pirch IRC clients. When it is executed, VBS.Funcess does the following: It determines whether it has already infected your computer by checking for the existence of the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Open

If the key does not exist, the worm copies itself to the \Windows\System folder as a random name with the extension .vbe. It then adds the \Open subkey to the following key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
so that the worm runs when you start Windows. Next it copies itself to the \Windows folder as Opel.vbs and searches all drives for folders that contain the files Mirc.ini or Pirch98.ini. If it finds these files, it creates the files Script.ini or Events.ini, respectively. These .ini files contain commands to send itself using the IRC client.

**VBS_FUNNY.D (Aliases: FUNNY.D, FUNNY, I-Worm.Veryfun, VBS/VeryFun) (Visual Basic Script Worm):** This worm propagates via e-mail by sending a message to addresses listed in an infected user's Microsoft Outlook address book. The e-mail arrives with the attachment "VERY FUNNY POLITICAL JOKE.TXT.VBS."

**W32/ElKern-B (Win32 Executable File Virus):** This is an executable file virus that works under Windows 98, Windows ME, Windows 2000 and Windows XP. It is capable of infecting file cavities. Under Windows 98 and Windows ME, W32/ElKern-B copies itself to the Windows System directory as the hidden file Wqk.exe, and sets the registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WQK,

to point to this file so that the virus runs every time the computer is rebooted. Under Windows 2000 and Windows XP, W32/ElKern-B copies itself to the Windows System directory as the hidden file Wqk.dll, and sets the registry key:

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Windows\AppInit_DLLs

to point to this file so that the virus runs every time the computer is booted. This virus is carried and dropped by the W32/Klez-E worm.

**W32.Fisp (Win32 Virus):** This virus is not a file infector. It spreads by copying itself to the folder in which it resides, using a random file name. When the virus is executed, it creates the text file \Windows\Spread_virus.txt. This file is just a log file that the virus uses to write the date and time of each random copy of itself that it creates. The virus sleeps for 10 minutes, and then it creates two randomly named copies of itself in the current directory and executes them. After the virus executes the two created files it exits. The other two created files that are running do the same thing. (They will sleep for 10 minutes, and each one will create two randomly named copies of itself in the current folder and executes them.) This process of execution is similar to a tree chart. The number of copies of the virus will double every 10 minutes. This will eventually crash the system or slow it down to a point where it will not function.

**W32.Klez.E@mm (Aliases: WORM_KLEZ.E, KLEZ):** This destructive mass-mailing worm can propagate copies of itself across network drives. Upon execution, it drops two executable files, WINK*.EXE and WQK.EXE, in the Windows System folder. It also creates registry entries that allow it to run at system startup. This worm terminates processes, and occasionally deletes files associated with certain antivirus programs.

**W32/Klez-F (Aliases: W32/Klez@mm,W32/Klez.F) (Win32 Worm):** This is a variant of W32/Klez-A and the functionality of W32/Klez-F is very similar to W32/Klez-E. It is a Win32 worm that carries a compressed copy of the W32/ElKern-B virus, which it drops and executes when the worm is run. This worm searches for e-mail address entries in the Windows address book but uses its own mailing routine with an attached file that is randomly named with extension .PIF, .SCR, .EXE or BAT. The sender address that appears in a message is chosen from a list inside the virus. W32/Klez-F attempts to disable several anti-virus products and delete some anti-virus related files. The worm attempts to exploit a MIME vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double-clicking on the attachment. Microsoft has issued a patch that secures against this vulnerability that can be downloaded from **www.microsoft.com/technet/security/bulletin/MS01-027.asp**. (This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this worm.) W32/Klez-F may also spread to remote shares on other machines using random filenames with a double extension. On remote shares, the worm will also create RAR archives and add itself. It copies itself to the Windows System directory with a random filename. The worm will set the registry key:

HKLM\Software\Microsoft\Windows\ CurrentVersion\Run\,

to point to the worm file, so that the file is run on Windows startup.

**W32/Maldal-F (Win32 Worm):** This is a worm that uses Microsoft Outlook to send itself to everyone in the Outlook address book. When first run the worm copies itself to the Windows folder as Christmas.exe and creates the registry entry:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Zacker = <Windows>\Christmas.exe

so that this file is run automatically each time the computer is restarted. The worm then disables the keyboard and also changes the computer name by setting the registry key:

HKLM\System\CurrentControlSet\Control\ComputerName\ComputerName\ComputerName = Zacker

and the default browser start page by setting, HKCU\Software\Microsoft\Internet Explorer\Main\Start Page.

**W32.TempX.A@m (Win32 Virus):** W32.TempX.A@m is a worm that is written in Visual Basic and is similar to many other Visual Basic worms that send themselves out by e-mail. It replicates only on Spanish versions of Windows.

**W97M.Doeii (Word 97 Macro Virus):** This is a macro virus that infects Microsoft Word documents and templates. This virus hooks the Microsoft Word event handlers in order to run its code. There is a one in 100 chance that a message that shows the name of the virus, as given by its author, will be displayed. There is a one in 100 chance that the virus will password protect the document with this password: "pietje."

**W97M/Pacol.a (Word 97 Macro Virus):** This virus infects Word 97 and Word 2000 documents. W97M/Pacol.a virus is a direct infector virus. It will set the security level to "Low" for Word 2000 and Word XP. The virus also creates the following files located in:

- C:\Windows\startm~1\programs\startup\winword.bat
- C:\Windows\winword.reg
- C:\Windows\normal.doc

The file winword.reg contains the code that modifies the registry settings for the security levels. Winword.bat is executed when Windows starts and executes the files C:\Windows\winword.reg and the infected C:\Windows\normal.doc. The virus will then search the hard disk and network drives for all .doc files found and overwrites itself to them. It will then do another search for all .txt, .wri and .pdf files and will overwrite itself to them and will add the .doc extension to these files. The original files will be deleted.

**WM97/Dig-C (Word 97 Macro Virus):** This is a variant of WM97/Dig-A. It creates the non-viral file ~WRr000^.tmp in the Temp directory, which it uses during replication. It may also display a message in Cyrilic characters.

**WM97/Fifteen-A (Word 97 Macro Virus):** This is a Word macro virus which, on the 15th or 30th of any month, will password protect infected documents with the password, >>xvx<<. The virus will also display a message box with the following characteristics if the user tries to access the Help|About menu option:

Title: >>>>>> XVX <<<<<<

Message: VIRUS INFECTED

**WM97/Marker-KC (Word 97 Macro Virus):** This is a corrupted but viable variant of WM97/Marker-C. Whenever a document is closed, the virus attempts to FTP user information from Word to the Codebreakers site and appends this information to the bottom of the macro as comments.

**WORM_BORMEX.A (Aliases: W32.Borm, I-Worm.Bormex, Win32/Bormex.A@mm, BORMEX.A, BORMEX):** Upon execution, this non-destructive, memory-resident worm appears as a hidden file. After execution, it sets itself in memory. If an infected user attempts to delete it, a message box is displayed saying "Access Denied."

**WORM_FRAGLED.A (Aliases: FAGLED.A, W32/Fagled@MM):** This worm is written in Visual Basic. It propagates via e-mail by collecting e-mail addresses from files with *.DBX, *.MBX, *.HTML, *.IDX, and *.VBS

extensions. It uses Microsoft Outlook's MAPI calls to send its e-mails. It also propagates via mIRC and Microsoft Messenger. It drops the file LED.EXE in the Windows directory.

**WORM_POPS.A (Aliases: POPS.A, POPS, W32/Pops.A@MM) (Win32 Worm):** This Win32 worm uses MAPI commands to propagate via e-mail. It arrives in an e-mail with the following:

Subject: cute worm
Message Body: the attached file is a compressed picture of a worm…click it..
Attachment: worm.com

The worm also drops a copy of WORM.COM in the root directory, C:\.

**WORM_SYSNOM.B (Aliases: SYSNOM.B, SYSNOM) (Internet Worm):** This Internet worm is created in Visual Basic and is UPX-compressed. It is capable of propagating via e-mail as an attachment. It does not have a destructive payload.

**X97M.ROH.A (Excel 97 Macro Virus):** This virus is written in macro language, and it infects Microsoft Excel worksheets. The virus spreads by first checking for the existence of the file \XLStart\Ft.xls. If the file does not exist, the virus creates the file -R¤H.xls in the XLStart folder. This file will be executed every time that Microsoft Excel starts. In some cases, this virus may remove some options from the Microsoft Excel menus. *Note: XLStart is the default name for the Microsoft Excel startup folder. The name of this folder can be changed from within Microsoft Excel. The virus will work even if this folder is named something other than XLStart.*

## Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be 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 # |
|---|---|---|
| Backdoor.Palukka | N/A | CyberNotes-2002-01 |
| **BackDoor-AAB** | **N/A** | **Current Issue** |
| DlDer | N/A | CyberNotes-2002-01 |
| **Hacktool.IPStealer** | **N/A** | **Current Issue** |
| JS/Seeker-E | N/A | CyberNotes-2002-01 |
| JS_EXCEPTION.GEN | N/A | CyberNotes-2002-01 |
| SecHole.Trojan | N/A | CyberNotes-2002-01 |
| Troj/Download-A | N/A | CyberNotes-2002-01 |
| Troj/Optix-03-C | N/A | CyberNotes-2002-01 |
| Troj/Sub7-21-I | N/A | CyberNotes-2002-01 |
| Troj/WebDL-E | N/A | CyberNotes-2002-01 |
| **TROJ_CYN12.B** | **N/A** | **Current Issue** |
| TROJ_DANSCHL.A | N/A | CyberNotes-2002-01 |
| **TROJ_FRAG.CLI.A** | **N/A** | **Current Issue** |
| **Trojan.Badcon** | **N/A** | **Current Issue** |
| **Trojan.StartPage** | **N/A** | **Current Issue** |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| **Trojan.Suffer** | **N/A** | **Current Issue** |

**BackDoor-AAB:** This Trojan claims to be a pre-release beta version of Sub7 2.3. It is actually a different backdoor which connects to an IRC server and accepts commands from there. The files that claim to be the client and edit server for this Trojan are also obvious decoys, which install the same remote-control component. The Trojan also appears to be able to use UPnP(Universal Plug and Play) vulnerabilities.

**Hacktool.IPStealer:** Hacktool.IPStealer is the detection for a collection of programs that a hacker can use to conceal intrusion and to obtain administrator-level access to Microsoft SQL Servers that have the default installation, in which the Administrator account has no password. It consists of the following seven programs:

- Sqlprocess.js
- Sqldir.js
- Run.js
- Sqlinstall.bat
- Clemail.exe
- Sqlscan.exe
- Sqlexec.exe

*Note: Clemail.exe is a shareware program and is not a Trojan.*

Microsoft SQL Server is vulnerable if it has the default installation where the administrator account has no password. Hacktool.IPStealer uses this vulnerability to send itself to other vulnerable Microsoft SQL Servers. When it is executed, Hacktool.IPStealer does the following:

- It scans randomly generated IP addresses on port 1433 in an attempt to find active Microsoft SQL Servers.
- Next it tries to add a user to the server and copy itself to the server using the default system administrator account. It also sends the server's IP address and some database information to the hacker's e-mail account.
- The Trojan also adds the registry key:
  HKEY_LOCAL_MACHINE\Software\Microsoft\Mssqlserver\Client\Connectto\Dsquery
  with the value, dbmssocn.

**TROJ_CYN12.B (Aliases: CYN12.B, Backdoor.Cyn.12.b):** This Aspack-compressed, client-server hacking tool is used to gain remote access to a compromised system. The server component (that runs on the infected user's computer) icon is that of a JPEG picture file. It is installed in the infected user's computer when the user executes the Trojan file. The server resides in the background. In Windows 9x systems, it is invisible in the task list. It opens and listens to TCP ports 113, 11225, and 22115, waiting for a connection from the client. When a connection is established, it allows the client program to send commands for it to process. To ensure execution at every system startup, it adds a registry run key in the registry as follows:

HKEY_LOCAL_MACHINE\Software\Windows\CurrentVersion\Run System32="\%Trojan filename%"

The hacker to control the server uses e client component. It is used by the hacker to connect to the installed server via a Graphical User Interface (GUI). There is also a supplementary tool used on the hacker side, to obtain the IP address of an infected computer, using the infected user's ICQ UIN (Unique Identification Number).

**TROJ_FRAG.CLI.A (Aliases: FRAG.CLI.A, FRAG):** This backdoor program is capable of producing a Server component that logs keystrokes, enables port connections, sends e-mails, or modifies the registry. It is non-polymorphic and is not memory-resident.

**Trojan.Badcon:** This is a Trojan horse that can cause unpatched Windows 95/98/98SE systems to crash and force a restart. The Trojan may present itself as a valid program, such as X-Box emulation software. It takes advantage of an

old Windows 95/98 vulnerability. A Microsoft patch that fixes this vulnerability has been available since March 2000. The affected systems are Windows 95, Windows 98 and Windows 98 Second Edition (SE). For details about this vulnerability and the patch, read the Microsoft Security Bulletin (MS00-017) located at: **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-017.asp**.

**Trojan.StartPage:** This is a Trojan horse that modifies the Internet Explorer home page without your permission. It may present itself as a valid program, and it may be Runtime compressed. When it is run, it changes the registry to set your Internet Explorer home page to a Web site that was chosen by the creator of the Trojan.

**Trojan.Suffer:** When the Trojan.Suffer Trojan horse is run, it displays a black box and repeatedly displays the word suffer in it. Each time that the word is displayed, the CD-ROM drive tray opens and closes. This is a Visual Basic-compiled executable that performs several functions before going into an infinite loop. The preparatory functions are:

- It swaps the mouse buttons.
- It hangs up any active RAS connections.
- It changes the computer name to something very rude.
- It registers the Trojan process as a service.
- It disables the use of the Control+Alt+Delete key combination.

The Trojan displays a black window and opens and closes the CD-ROM drive tray. With each opening and closing of the tray, it displays the following in red text: "suffer..." If you place the mouse pointer over the black window, and do not move the mouse, the following pop-up description is displayed:

"You got caught slippin', now that ass is mine..."